

Service Hardware

SLA	Description	Response Time	Resolution Time	Total Time
Hardware Request	(e.g. pcs, laptops, local printer, scanner, blackberry, etc.)	0 hours up to 8 hours	16 hours	3 days
Hardware Request Other	(e.g. external hard drives, external card readers) All Pending approval	0 hours up to 16 hours	16 hours	4 days
Hardware Failure	(e.g. pcs, laptops, local printer, scanner, blackberry)	0 hours up to 4 hours	8 hours	2 days
Network Printer Failure	Service Interruption (Times may be affected by vendor availability)	0 hours up to 8 hours	16 hours	3 days

Service VOIP

SLA	Description	Response Time	Resolution Time	Total Time
VM Request/Call Center Agent	VM Request / Call Center Agent	0 hours up to 8 hours	4 days	5 days
Phone	Phone replacement, move or add a phone to an existing line	0 hours up to 8 hours	4 days	5 days
Circuit (Analog, Fax, ISDN)	Move existing line or add new line to an existing outside circuit	0 hours up to 8 hours	7 days	8 days
Call Forwarding	Request for Call Forwarding	0 hours up to 8 hours	4 days	5 days
Audio Conference/Calling Card	Request for Audio Conference/ Calling Card			
VOIP Failure	Service interruption	0 hours up to 8 hours	4 days	5 days

Service Desktop Applications

SLA	Description	Response Time	Resolution Time	Total Time
Desktop software applications Failures	Standard applications (Outlook, Office Suite, Adobe, IE, Firefox, Chrome, Roxio, Project, Access, Visio, etc.)	0 hours up to 4 hours	8 hours	2 days
Desktop software applications Standard Requests	Standard applications (Outlook, Office Suite, McAfee, Adobe, IE, Firefox, Chrome, Roxio, Project, Access, Visio, etc.)	0 hours up to 8 hours	16 hours	3 days
Desktop software applications non-standard Requests	Non-Standard (Dragon Naturally Speaking, Initiator, AutoCAD, Adobe CSX, etc)	0 hours up to 16 hours	16 hours	4 days

Service Web Applications

SLA	Description	Response Time	Resolution Time	Total Time
Web Application Access	(e.g. CBS, Sunflower, WebTA, WebflowDoc, Accelion)	0 hours up to 16 hours	16 hours	4 days
Web Application Failure	(e.g. CBS, Sunflower, WebTA, WebflowDoc, Accelion)	0 hours up to 8 hours	16 hours	3 days

Service Server Applications

SLA	Description	Response Time	Resolution Time	Total Time
Server Application Failure	(e.g. BES, Active Directory, Safeboot, Endpoint, Exchange)	0 hours up to 2 hours	8 hours	1 day
Password Reset	(e.g. Windows Password Reset, Safeboot, Endpoint, etc)	0 hours up to 1 hours	4 hours	8 hours

Service Network

SLA	Description	Response Time	Resolution Time	Total Time
Routine Network Requests	Routine Firewall changes, Port Activation from an existing line	0 hours up to 8 hours	4 days	5 days
Wi-Fi Failure for GFE ONLY	Unable to connect	0 hours up to 8 hours	4 days	5 days
Non-Routine Network Requests	non-Routine Firewall, DHCP, DNS, Site-to-Site VPN changes	0 hours up to 8 hours	11 days	12 days
Network Failures	Firewall, Port Activation, Circuit request, Site to Site VPN, etc	0 hours up to 8 hours	4 days	5 days
New Port Activation	Run a new cable from the customer to an existing switch and activate port	0 hours up to 8 hours	7 days	8 days

Service Remote Access

SLA	Description	Response Time	Resolution Time	Total Time
Remote Access Request	(e.g. new remote access connection, IPSEC or SSL)	0 hours up to 8 hours	2 days	3 days
Remote Access Failure	(e.g. connection)	0 hours up to 8 hours	2 days	3 days
Password / PIN Reset	(e.g. RSA Token Reset)	0 hours up to 4 hours	8 hours	2 days


Service Employee Actions

SLA	Description	Response Time	Resolution Time	Total Time
Setup/Departure	New Employee or Employee Departure	0 hours up to 8 hours	16 hours	3 days
Access Requests	(e.g. calendar, file share, mail increase, name change,	0 hours up to 2 days	4 days	6 days
Move	(e.g. CD-410s, reconnect/disconnect equipment, ports)	0 hours up to 2 days	4 days	6 days



UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

SEP 12 2014

MEMORANDUM FOR: Chief Information Officers
FROM: Steven I. Cooper 
SUBJECT: 2014 DOC Information Technology Security Program Policy

I am pleased to introduce the 2014 DOC Information Technology Security Program Policy (ITSPP), effective immediately. This policy update is the result of a collaborative Department-wide effort to align DOC IT security policies with current federal and DOC directives, regulations, requirements and standards.

OUs are required to comply with the DOC ITSPP within 120 days. Compliance with the DOC ITSPP beyond the specified timeframe shall be managed through the use of Plans of Action and Milestones (POA&Ms).

Please contact DOC IT Security Policy Program Lead, Patty McMahon, at pmcmahon@doc.gov or (202) 482-1898 with questions or for additional information.

Cc DOC Chief Information Security Officer
DOC IT Security Coordinating Committee (ITSCC)

U.S. DEPARTMENT OF COMMERCE



Department of Commerce

Information Technology Security Program Policy

Version: 3.2

September 2014

**Prepared by:
Office of Cyber Security IT Security Policy Team**

Change/Review Record

Modifications made to this document are recorded in the Change/Review Record below. Reviews made as part of the assessment process should also be recorded below. This history shall be maintained throughout the life of the document.

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes Made by Name/Title/Organization
1.0	June 30, 2005	Version 1.0 released		DOC OCIO
2.0	January 2009	Revised version 2.0 released		DOC OCIO
3.0	February 2014	Transferred 2.0 to new template	All	OCS
3.1	July 21, 2014	Compiled Sections 1 and 2 of ITSPP for DOC Union Review	All	OCS
3.2	Sept 2, 2014	Final Revision for CIO Review		OCS

Table of Contents

1	Introduction	1
1.1	Background	1
1.2	Purpose	1
1.3	Scope and Applicability	1
1.4	IT Security Documentation	2
1.5	ITSPP Organization.....	2
2	Policy	4
2.1	Effective Date.....	4
2.2	Scoping and Waivers.....	4
2.2.1	Control Tailoring (Scoping).....	4
2.2.2	Waivers	5
2.3	Enforcement	5
3	IT Security Roles and Responsibilities.....	7
3.1	DOC Personnel.....	7
3.2	DOC Senior Officials	7
3.2.1	Secretary of Commerce.....	7
3.2.2	DOC Chief Information Officer (CIO)	7
3.2.3	DOC Chief Information Security Officer (CISO)/SAISO	8
3.2.4	DOC Director of the Office of Cyber Security (OCS).....	9
3.2.5	DOC IT Security Compliance & Risk Management Officer (CRMO).....	9
3.2.6	DOC Critical Infrastructure Protection Manager (CIPM).....	9
3.2.7	DOC Director for Security	9
3.2.8	DOC Chief Privacy Officer.....	10
3.2.9	Privacy Program Coordinator	10
3.2.10	DOC Deputy Chief Privacy Act/Freedom of Information Act (FOIA) Officer.....	10
3.3	Operating Unit (OU) Roles	10
3.3.1	Risk Executive (Function)	11
3.3.2	OU Chief Information Officer (CIO).....	11
3.3.3	Information Owner/Steward	12
3.3.4	OU Privacy Act Officer/Freedom of Information Act (FOIA) Officer.....	12
3.3.5	OU (Bureau) Privacy Officers	12
3.3.6	OU Information Technology Security Officer (ITSO)/OU CISO/SAISO	12

3.3.7	Authorizing Official (AO)/Co-Authorizing Official (Co-AO)	13
3.3.8	Authorizing Official Designated Representative (AODR)	14
3.3.9	Common Control Provider (DOC or OU-level)	14
3.3.10	System Owner (SO)	15
3.3.11	Information System Security Officer (ISSO)	15
3.3.12	Security Controls Assessor (SCA)	15
3.3.13	Additional Roles	16
3.3.13.1	Contracting Officer (CO)	16
3.3.13.2	Contracting Officer's Technical Representative (COTR)	16
3.3.13.3	Supervisor	17
3.3.13.4	Account, Application, Database, Network and System Administrators	17
3.3.13.5	Developers and Programmers	17
3.3.13.6	Key Contingency Roles	17
3.3.13.7	IT Security Incident Response Personnel	18
3.3.13.8	Users	18
3.4	Commerce IT Groups	18
3.4.1	CIO Council	19
3.4.2	Commerce IT Review Board (CITRB)	19
3.4.3	Enterprise Architecture (EA) Advisory Group	19
3.4.4	IT Security Coordinating Committee (ITSCC)	19
3.4.5	Web Advisory Council (WAC)	19
3.4.6	Electronic and IT (EIT) Accessibility Coordinator and Commerce Information Quality Task Force	19
3.4.7	Federation of Computer Incident Response Teams (FedCIRTs)	20
3.4.8	Commerce Capital Planning and Investment Control (CPIC) Community	20
3.4.9	HSPD-12 Working Group	20
3.4.10	IT Audit Working Group	20
3.4.11	DOC Privacy Council	20
3.4.12	DOC PII Breach Response Task Force	21
3.5	DOC Offices	21
3.5.1	Office of the Chief Information Officer (OCIO)	21
3.5.2	Office of Cyber Security (OCS)	21
3.5.3	Office of Security (OSY)	22

3.5.4	Office of Acquisition Management (OAM).....	22
3.5.5	Office of Human Resources Management (OHRM).....	24
3.5.6	Office of Inspector General (OIG).....	25
3.5.7	Office of General Counsel (OGC)	25
3.5.8	Office of Privacy and Open Government (OPOG).....	25
4	Baseline Security Controls	26
4.1	Security Control Policies and Procedures	26
4.2	Security Control Catalog Key	27
4.3	Access Control (AC)	27
4.4	Security Awareness and Training (AT)	31
4.5	Audit and Accountability (AU).....	32
4.6	Security Assessment and Authorization (CA)	33
4.7	Configuration Management (CM).....	34
4.8	Contingency Planning (CP).....	36
4.9	Identification and Authentication (IA).....	37
4.10	Incident Response (IR)	38
4.11	Media Protection (MP)	40
4.12	Physical and Environmental Protection (PE)	40
4.13	Planning (PL).....	41
4.14	Personnel Security (PS).....	42
4.15	Risk Assessment (RA).....	44
4.16	System and Services Acquisition (SA).....	45
4.17	System and Communications Protection (SC)	47
4.18	System and Information Integrity (SI).....	47
4.19	Program Management (PM)	49
	Appendix A: Acronyms and Abbreviations.....	52
	Appendix B: Glossary.....	55

1 Introduction

The Department of Commerce (DOC) is strongly committed to Information Technology (IT) Security. DOC leaders at all levels recognize that security must be inherent in our business processes and IT systems to support the various missions and service functions of the organizations. Given the significant and growing danger of current cyber threats, DOC managers systematically recognize and manage information security-related risks and take steps to understand these risks to achieve more secure information and information systems through the implementation of appropriate risk mitigation strategies. This is important, not only to achieve adequate compliance with public laws, federal regulations, and standards, but also to aid in the DOC mission to foster, promote, and develop the foreign and domestic commerce of the United States. This document sets forth the DOC Information Technology Security Program Policy (ITSPP), which specifies IT security and privacy requirements to meet the minimum legal and federal mandates for information security.

1.1 Background

The DOC mission impacts industry, federal agencies, local, tribal, state, and international governments, and the American people in many ways. The work on behalf of these constituents is either directly or indirectly reliant on the confidentiality, integrity, and availability of DOC information and information systems. IT security supports the DOC mission by ensuring our information and information systems are protected against risks of loss, misuse, or unauthorized access in accordance with applicable laws.

1.2 Purpose

The DOC ITSPP specifies the mandatory requirements for the DOC IT Security Program. This policy addresses requirements and guidance set forth by the Federal Information Security Management Act (FISMA) and provides clarity on the Department's specific control parameters. It also encompasses minimum security controls as required by Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, defined by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and commensurate with the security categorization defined by FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

1.3 Scope and Applicability

The DOC ITSPP applies to all Operating Units (OUs) and employees (federal and contractor), guest researchers, collaborators, and others requiring access to DOC information systems. This policy also applies to organizations and services to which DOC and/or OUs have contracts or legal agreements. The DOC ITSPP applies to all IT systems owned or operated on behalf of DOC. Requirements apply also to systems which are not owned by DOC but to which DOC interconnects and has legal and/or contractual authority to dictate requirements. The term

Information Technology Security encompasses all requirements for information security (i.e., protection of data) as well as the requirements necessary to maintain the confidentiality, integrity, and availability of the Departments information technology infrastructure. Classified information and information systems are not within the scope of this document.

1.4 IT Security Documentation

The DOC ITSPP includes policy statements, NIST SP 800-53 Rev. 4 security controls requiring DOC-specific parameters, and supporting criteria for controls where specificity is warranted. OUs are responsible for following NIST SP 800-53 Rev. 4 for implementing control details that are not explicitly described in the ITSPP.

The DOC ITSPP is comprised of the body of the document itself as well as the following documents, which supplement the minimum implementation standards described herein and carry authority equal to the DOC ITSPP:

- Commerce Information Technology Requirements (CITRs): CITRs are a fundamental component of the DOC ITSPP. CITRs are released as new threats arise or federal mandates are introduced that require the implementation of additional IT security measures. CITRs are real-time updates that amend or supersede the current version of the DOC ITSPP. Like the ITSPP, CITRs shall be reviewed by the DOC IT Security Coordinating Committee (ITSCC), and Chief Information Officer (CIO) Council, as necessary, and approved by the DOC CIO;
- Policy Memoranda: Policy memoranda contain security directives, advisories or information that do not necessarily fit into the scope of the DOC ITSPP but are required for implementation across the Department; and
- Frequently Asked Questions (FAQs): FAQs are released to provide clarification on requirements outlined in the DOC ITSPP, CITRs and policy memoranda. Recommendations or best practices are specifically noted and separated from official policy statements within the FAQs. These are included for informational purposes but are not required by policy.

The DOC ITSPP, CITRs, policy memoranda, FAQs and other related documentation can be found on the DOC OCIO IT Security Policy and FISMA Reporting Team Intranet site. Comments or questions regarding the DOC IT Security Program documentation can be submitted via e-mail to DOCITSecurity@doc.gov.

1.5 ITSPP Organization

The DOC ITSPP is divided into six (6) sections:

- Section 1 - Introduction, which describes the background, purpose, scope and applicability, and documentation;
- Section 2 - Policy, which describes the policy authority, effective date, scoping and waivers, and enforcement;

- Section 3 - IT Security Roles and Responsibilities, which provides an outline of the DOC offices, DOC/OU roles, and DOC IT groups that play a role in implementing DOC ITSPP requirements;
- Section 4 - Baseline Security Controls contains a list of security controls requiring a DOC parameter or DOC-specific criteria;
- Appendix A – Acronyms and Abbreviations; and
- Appendix B – Glossary.

2 Policy

DOC OUs must develop, document, and implement an IT Security Program to protect the confidentiality, integrity, and availability of DOC information and information systems in accordance with the Federal Information Security Management Act of 2002 (FISMA) and other applicable legislation.

DOC OUs must use FIPS 199 to categorize information systems and determine their appropriate impact levels (Low, Moderate, or High). OUs must select the security controls baseline defined in NIST SP 800-53, Rev. 4 based on the system's impact level, and tailor, supplement, and implement the baseline according to NIST SP 800-53, Rev 4. OUs must use NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* (pending final release of NIST SP 800-53A, Revision 2) as the basis for assessing information system security controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. OUs must assess and authorize information systems in accordance with DOC CTR-019, *Risk Management Framework* and NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

2.1 Effective Date

The DOC ITSPP is effective upon issuance and supersedes the 2009 DOC ITSPP.

OUs are required to comply with the DOC ITSPP within 120 days. Effective dates of other policy vehicles (e.g. CTRs, policy memos, and FAQs) will be specified in each respective policy vehicle. Compliance with the DOC ITSPP beyond the specified timeframe shall be managed through the Plan of Action and Milestones (POA&Ms).

The DOC Chief Information Security Officer (CISO)/Senior Agency Information Security Officer (SAISO) will review the DOC ITSPP at least annually and incorporate updates as necessary. The revised DOC ITSPP shall be reviewed by the DOC ITSCC and CIO Council, as necessary, and approved by the DOC CIO.

2.2 Scoping and Waivers

2.2.1 Control Tailoring (Scoping)

DOC OUs have the flexibility to tailor security control baselines in accordance with the terms and conditions set forth in NIST SP 800-53 Rev. 4, Chapter 3.2: "Tailoring Baseline Security Controls." Scoping provides specific terms and conditions on the applicability and implementation of NIST SP 800-53 Rev. 4 security controls. In addition, scoping may also be applied to controls and parameters that fall outside of the NIST SP 800-53 Rev. 4 framework (e.g. DOC Criteria) and for which waivers are not required by OU CIOs. Questions regarding controls and parameters can be submitted to the DOC CISO/SAISO.

Implementation details for all controls being employed on the system must be stated in the

system's System Security Plan (SSP). Controls the Authorizing Official (AO) has elected not to employ as a result of following the scoping guidance in NIST SP 800-53 Rev. 4, or because the AO has deemed the control technically or operationally infeasible to implement must have the following information documented for each control not being employed:

1. Explanation of circumstance justifying foregoing the implementation of the control (SSP- field for that specific control);
2. Description of all compensating controls reducing the risks associated with the inability to implement the control (SSP-field for that specific control);
3. Description of any residual risk introduced as a result of not implementing the control (Risk Assessment); and
4. Controls not currently being employed but which are planned to be employed must be documented in a POA&M and the POA&M referenced in the respective control section in the SSP or Risk Assessment.

2.2.2 Waivers

Waivers are to be adjudicated by the OU CIO, except for controls and/or policies that explicitly require a waiver be adjudicated at the DOC CIO level. Compliance with collective bargaining agreements and labor relations laws constitute legitimate grounds for OUs to grant waivers to security requirements. Circumstances for waivers differ from controls baseline tailoring as described in Section 2.2.1 above, in that waivers are to be provided for instances of widespread (affecting multiple OU systems or users) inability to implement certain policy requirements or in situations where policies explicitly require a waiver for a specific control or requirement. Waiver requests must document, as applicable:

1. Explanation of unique circumstance justifying foregoing the implementation of the requirement/control;
2. Description of compensating controls that provide an equivalent or comparable protective value to that of the requirement/control not being implemented;
3. Description of any residual risk introduced as a result of not implementing the requirement/control;
4. Documented POA&Ms for controls not currently being employed but which are planned; and
5. Decision by the OU CIO (or DOC CIO in cases where policy requires DOC CIO approval of waivers).

Waivers must be referenced in relevant system security documentation (e.g., SSP and Risk Assessment) and made available to the DOC CISO/SAISO upon request.

2.3 Enforcement

The DOC ITSPP and CITRs are issued under the authority of the Department Administrative Order (DAO) 200-0, *DOC Handbooks and Manuals* as a section of the IT Management Handbook, and thereby have the same force and effect as a DAO.

Violations of the DOC ITSPP and/or CITRs may result in loss of IT access, disciplinary action, or other consequences consistent with DAO 202-751, *Discipline*, and/or civil or criminal action against the offending employee(s), associate(s), and/or contractor(s), consistent with applicable law, or contract terms as applicable.

3 IT Security Roles and Responsibilities

The responsibility to protect DOC information and technological resources extends to all non-public users and requires collaboration across various offices to coordinate activities associated with DOC's security posture, technological environment, and overall risk management.

3.1 DOC Personnel

All of the responsibilities and requirements delineated by the DOC ITSPP apply to any individual performing a security role as described below, regardless of employer. Additional security requirements that are not within the scope of this document are described in the DOC Manual of Security Policies and Procedures.

3.2 DOC Senior Officials

The roles in this section are carried out by individuals at the Departmental level. DOC Senior Officials are responsible for the day-to-day management and general supervision of their respective programs and/or OUs.

3.2.1 Secretary of Commerce

The Secretary of Commerce is responsible for ensuring the DOC information and information systems are protected in accordance with directives from the Office of Management and Budget (OMB), Congress, and as set forth in Presidential Directives (PDs).

3.2.2 DOC Chief Information Officer (CIO)

The responsibilities of the DOC CIO are specifically defined in Departmental Organization Order (DOO) 15-23, Chief Information Officer.

The DOC CIO also performs the following duties:

- Leads the management of information resources throughout the Department, ensuring that the Department's programs make full and appropriate use of information technology;
- Monitors and evaluates the performance of IT programs on the basis of applicable performance measurements and advise the Secretary/Deputy Secretary regarding whether to continue, modify, or terminate a program or project;
- Designates in writing, a DOC CISO/SAISO, to execute the IT Security Program to assure the confidentiality, integrity, and availability of information and IT resources, with information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access for national and non-national security systems;
- Develops, maintains, and facilitates the implementation of a Strategic IT Plan and an Enterprise IT Architecture for the Department;
- Approves and issues DOC policies and other guidance for the management of information resources throughout the Department, and monitor and enforce compliance with such policies and guidance;

- Monitors, evaluates, and reports to the Secretary of Commerce on the status of IT security within the Department;
- Serves as the Department's Chief Infrastructure Assurance Officer (CIAO) to carry out the critical infrastructure protection policies provided in Presidential Decision Directive 63 of May 22, 1998, and support implementation of the Department's Critical Infrastructure Protection Program;
- Carries out the Secretary's responsibilities under OMB Circular A-130, "Management of Federal Information Resources"; and
- Serves as Chair of the Commerce CIO Council to promote effective IT management practices throughout the Department and share information of a crosscutting nature.

3.2.3 DOC Chief Information Security Officer (CISO)/SAISO

The DOC CISO is the Senior Agency Information Security Officer (SAISO) who directs the management of the Department's IT Security Program. The DOC CISO/SAISO, with the support of DOC Senior Officials, establishes a strong foundation for DOC IT security by interacting with internal and external resources, and coordinating IT security compliance across DOC OUs.

The DOC CISO/SAISO coordinates with the DOC CIO, Director of the Office of Cyber Security (OCS), the Compliance and Risk Management Officer (CRMO), the Critical Infrastructure Protection Manager (CIPM), OU ITSOs, Information Technology Security Coordinating Committee (ITSCC) and OU CIOs to:

- Develop, document, and implement the DOC IT Security Program to provide information security for the electronic information and information systems that support the operations and assets of the DOC including those provided or managed by another agency, contractor, or other source, that includes:
 - Develop and maintain IT security policies, plans, control techniques and procedures for information systems, to include developing related standards to be followed by the OU, and developing standards, procedures, and practices to establish an IT Security Program as an integral part of the IT Management Program;
 - Inform personnel of training requirements (i.e., IT Security Awareness Training) to access information systems that support the operations and assets of the DOC;
 - Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities;
 - Define activities associated with Security Assessment and Authorization (A&A), including configuration management, security assessment, and implementation of enterprise-wide tools; and
 - Oversee required IT Security reporting activities to external and internal entities.
- Plan and co-chair regular meetings of the IT Security Coordinating Committee (ITSCC) as a forum for exchange and action on Department-wide IT security practices, guidance and policies; and
- In coordination with SHRO, OSY, and OAM, review and revise position risk designations on a sampling basis at least annually and as position functions change.

3.2.4 DOC Director of the Office of Cyber Security (OCS)

The DOC Director of the OCS coordinates with the DOC CIO, CISO/SAISO, CRMO, CIPM and OU CIOs to:

- Ensure IT security is included in the DOC Strategic IT Planning and Enterprise Architecture (EA) efforts; and
- Identify IT security resource requirements for the Department. Each OU CIO or equivalent will ensure that funds and personnel needed to manage the IT Security Program are adequately addressed within their OU.

3.2.5 DOC IT Security Compliance & Risk Management Officer (CRMO)

The DOC CRMO coordinates with the DOC CIO, CISO/SAISO, Director of OCS, CIPM, and OU CIOs to:

- Monitor and evaluate the status of the DOC IT Security posture by performing annual compliance reviews of OU IT Security Programs;
- Advise the DOC CIO and OU CIOs of technological IT security advances that can be used on a Department-wide scale and provide reduced costs for IT security efforts; and
- Report to the DOC CIO and external entities, such as OMB, Government Accountability Office (GAO), and Congress, on IT Security Program status within the Department.

3.2.6 DOC Critical Infrastructure Protection Manager (CIPM)

The responsibilities of the DOC CIPM encompass establishment, coordination, and implementation of all activities associated with the protection of Critical Infrastructure, including the IT component of Continuity of Operations Planning (COOP).

The CIPM coordinates with the DOC CIO, CISO/SAISO, Director of OCS, CRMO, CIPM, and OU CIOs to:

- Develop the DOC Critical Infrastructure Protection (CIP) Program, including providing the Director of the OCS with input on policies and procedures for (i) incident response capability, (ii) the IT component of COOP;
- Act as the DOC liaison with United States Computer Emergency Readiness Team (US-CERT), and manage DOC Federated Computer Incident Response Program; and
- Identify resource requirements, including funds, personnel, and contractors, needed to manage the CIP Program.

3.2.7 DOC Director for Security

The DOC Director for Security, as defined by DOO 20-6, *Director for Security*, Section 5 coordinates with the DOC CIO, CISO/SAISO, Director of OCS, CRMO, CIPM, and OU CIOs to:

- Develop and enforce appropriate physical security controls;

- Serve as the principal Departmental official for coordinating and assisting in the establishment and continuation of a Department-wide emergency action program, to include emergency preparedness, particularly as applicable to the requirements of EO 12656, Assignment of Emergency Preparedness Responsibilities;
- Identify and address the physical security needs of computer installations, office environments, and backup installations;
- Process and maintain personal background checks and security clearance records;
- Issue Identification (ID) badges to DOC personnel at the Office of Security (OSY) controlled Credentialing Centers and Common Access Card (CAC) stations in accordance with Homeland Security Presidential Directive-12 (HSPD-12);
- Serve as the Department's liaison with agencies of federal, state, and local government in security, executive protection, and Departmental counterintelligence issues; and
- Conduct investigations under the authorities, functions, and responsibilities of OSY.

3.2.8 DOC Chief Privacy Officer

The DOC Chief Privacy Officer functions as the Executive Director for the Senior Agency Official for Privacy (SAOP), having overall responsibility and accountability for ensuring the agency's implementation of information privacy protections and the development and evaluation of legislative, regulatory, and other policy proposals which involve information privacy issues, consistent with the responsibilities under the E-Government Act of 2002 and FISMA.

3.2.9 Privacy Program Coordinator

The Privacy Program Coordinator reports directly to the Chief Privacy Officer and serves as the primary point of contact for OU (Bureau) Privacy Officers for the review, coordination, and analysis of personally identifiable information (PII) breaches and privacy impact assessments (PIAs), ensures PII breach incident reports follow guidelines established in the "Department of Commerce PII, Business Identifiable Information, and Privacy Act Breach Response and Notification Plan," and provides assistance in the development of policies, regulations, procedures, and guidelines relating to PII breach incident reporting, and approval of PIAs.

3.2.10 DOC Deputy Chief Privacy Act/Freedom of Information Act (FOIA) Officer

The Deputy Chief Privacy Act/Freedom of Information Act (FOIA) Officer develops and oversees the implementation of Department-wide policies and procedures relating to the Privacy Act and administration of FOIA, assures that personal information contained in a Privacy Act system of records is handled in compliance with its provisions, and manages the Department's FOIA process and implements programs required by FOIA for providing public access to Departmental records and information.

3.3 Operating Unit (OU) Roles

This section describes the core security-related responsibilities for senior officials and information and/or system owners within DOC OUs. More comprehensive descriptions and

additional security roles can be found in NIST SP 800-37. Not all roles listed in this section will apply to all OU information systems.

The head of each OU or departmental office, in consultation with the Servicing Human Resources Office (SHRO), must ensure that each position is designated at the appropriate level of sensitivity and/or risk in accordance with the DOC Manual of Security Policies and Procedures, Chapter 10. Heads of OUs assign responsibilities based on management responsibility. They also ensure that this designation is clearly stated in the position description so that OSY can perform the appropriate background investigation. Future changes in responsibilities or delegations may involve changes in working conditions that should not be made before required bargaining with appropriate organizations occurs.

3.3.1 Risk Executive (Function)

The risk executive (function) is an individual or group within an organization that helps to ensure that: (i) risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success. This function may be retained by the head of the agency/organization or delegated to another official or group (e.g., an executive leadership council).

If there is a risk executive (function) role, the individual or group are to be U.S. government personnel only.

3.3.2 OU Chief Information Officer (CIO)

OU CIOs examine the interdependencies and interconnections of IT resources and provide for the separation of duties, including sufficient supervision and coordination among System Owners (SOs).

The OU CIO coordinates with the DOC CIO, CISO/SAISO, Director of OCS, CRMO, and CIPM to:

- Oversee the management of the OU IT Security Program and approve OU supplements to the DOC ITSPP;
- Appoint, in writing, an OU CISO/ SAISO/ ITSO to implement the IT Security Program; and
- Serve as the AO or Co-AO, as necessary, for unclassified systems within the OU.

The following OU CIO responsibilities may be delegated to the OU CISO/SAISO/ITSO as necessary:

- Manage the OU IT Security Program;
- Develop, maintain, and oversee the OU IT Security Policy;
- Ensure that IT security policies are developed and approved;

- Ensure the implementation of the IT Security Program complies with FISMA, which includes independent evaluations of the program;
- Provide overall management of and leadership and direction to the IT Security Program;
- Report the status of the IT Security Program to the DOC CRMO, and any weaknesses of the program;
- Ensure that the IT Security Planning is done throughout the life cycle of the system;
- Ensuring that all IT resources are identified, including complying with the Department's capital asset budget planning process and following a methodology consistent with NIST SP 800-65, *Integrating IT Security into the Capital Planning and Capital Investment Control Process*, and making IT security explicit in IT investments and capital programming;
- Train and oversee personnel with significant responsibilities for information security; and
- Provide feedback to the Department on the status of the program in the OU as required by FISMA, and suggest improvements or areas of concern in the OU program or any other Departmental program or activity; and,

3.3.3 Information Owner/Steward

The information owner/steward is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. The owner/steward of the information processed, stored, or transmitted by an information system may or may not be the same as the system owner. A single information system may contain information from multiple information owners/stewards. Information owners/stewards provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted.

3.3.4 OU Privacy Act Officer/Freedom of Information Act (FOIA) Officer

Each OU Privacy Officer/FOIA Officer or equivalent is responsible for providing information on procedural issues involving the Privacy Act and addressing privacy concerns relative to their individual OU. The Office of General Counsel (OGC) provides guidance on all legal issues involving the Privacy Act.

3.3.5 OU (Bureau) Privacy Officers

The OU (Bureau) Privacy Officers provide oversight on the implementation of privacy policies, procedures, and guidance within the OUs and ensure effective execution of breach responses.

3.3.6 OU Information Technology Security Officer (ITSO)/OU CISO/SAISO

The OU ITSO is the CISO/SAISO appointed by the OU CIO. An OU CISO/SAISO is responsible for ensuring that the appropriate operational security posture is maintained for information systems and programs under their OU's control. The OU CISO/SAISO reports to

the DOC CISO/SAISO, through the OU CIO. In contrast, within NOAA, a NOAA Line Office (LO) ITSO has responsibility for the IT Security Program within their major subordinate component. The OU CISO/SAISO serves as the principal advisor to the AO, SO, NOAA LO ITSO and DOC CISO/SAISO on all matters (technical and otherwise) involving the security of the OU's IT systems, and maintains copies of artifacts required for security authorization (as described in CTR-019: *Risk Management Framework*). Additionally, the OU CISO/SAISO/ITSO must:

- Develop and maintain the OU IT Security Policy, procedures, standards, and guidance consistent with Departmental and Federal requirements;
- Conduct continuous monitoring of the OU's IT Security Program annually to ensure effective implementation of, and compliance with, established policies and procedures;
- Establish a process to ensure that all users are provided annual information system security training, copies of Rules of Behavior (RoB), and are trained to fulfill their IT security responsibilities including procedures for general and specialized training;
- Notify SOs of user infractions identified during routine compliance assessments;
- Participate as a voting member of the ITSCC, participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate;
- Coordinate with the Director of the OCS, OU CIO and CIPM, as appropriate, concerning incidents and potential threats; and
- Complete the DOC IT Compliance in Acquisition Checklist or a materially similar checklist in coordination with the following individuals, as appropriate: Cognizant OCIO, Cognizant OCIO Representative, OU COTR, OU ISSO, OU-approved Program/Requesting Office IT Security Officer, and CO.

As appropriate, the ITSO/SAISO may also take on the responsibilities of the Information System Security Engineer and Information Security Architect roles, as described in NIST SP 800-37.

3.3.7 Authorizing Official (AO)/Co-Authorizing Official (Co-AO)

The AO is a senior official or executive with the authority to assume responsibility for operating an information system at an acceptable level of risk to operations, assets, or individuals by granting an Authorization to Operate (ATO) or Deny Authorization to Operate (DATO) as defined in NIST SP 800-37. The role of Co-AO is the OU CIO for their respective OU. AOs/Co-AOs must have the authority to oversee the budget and business operations of the information system within the DOC. The AO approves system security requirements, System Security Plans (SSPs), Interconnection Security Agreements (ISAs), and Memorandums of Agreements (MOAs) and/or Memorandums of Understanding (MOUs).

The AO is also ultimately responsible for ensuring continued ATOs for systems under their responsibility by reaffirming acceptable Continuous Monitoring results and reassessing, documenting, and accepting risks at least annually for systems that fall under their responsibility. Reaffirmation of the ATO must be documented in writing, either by signing off on acceptable assessment results or by signing a Reauthorization Memo, and entered into the Cyber Security

Assessment and Management (CSAM).¹

With the increasing complexities of missions and organizations, a particular information system may have multiple AOs. If so, agreements must be established among the AOs and documented in the SSP.

The Authorizing Official role has inherent U.S. Government authority and is assigned to government personnel only.

3.3.8 Authorizing Official Designated Representative (AODR)

The authorizing official designated representative is an organizational official that acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process. Authorizing official designated representatives can be empowered by authorizing officials to make certain decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk. The designated representative may also be called upon to prepare the final authorization package, obtain the authorizing official's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials. The only activity that cannot be delegated to the designated representative by the authorizing official is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation).

3.3.9 Common Control Provider (DOC or OU-level)

The common control provider is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). Common control providers are responsible for: (i) documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization); (ii) ensuring that required assessments of common controls are carried out by qualified Security Control Assessors (SCAs) with an appropriate level of independence defined by the organization; (iii) documenting assessment findings in a security assessment report; and (iv) producing a plan of action and milestones for all controls having weaknesses or deficiencies. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) is made available to information system owners inheriting those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls. The common control provider notifies system owners of any status changes to the common controls that may impact the security of their systems.

¹ Formerly referred to as the DOC FISMA reporting system.

3.3.10 System Owner (SO)

The responsibility of the SO, as defined by NIST SP 800-37, is the overall procurement, development, integration, modification, operation, security and maintenance of an information system. As specified in DOC CTR-019: *Risk Management Framework*, the SO must be identified on the list of key system stakeholders that is included in the required artifacts for initial system authorization.

The SO is responsible for the development and maintenance of the SSP and ensures the system is deployed and operated according to the agreed-upon security requirements. The SO is also responsible for deciding who has access to the information system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in RoB). The SO informs key agency officials of the need to conduct a security A&A of the information system, ensures that appropriate resources are available for the effort, and provides the necessary system-related documentation to the SCA. The SO manages risk by taking appropriate steps to reduce or eliminate vulnerabilities and ensures the AO or AODR are provided with enough information to make risk-based decisions prior to adjudication.

3.3.11 Information System Security Officer (ISSO)

The responsibility of the ISSO is to ensure the appropriate operational security posture is maintained for an information system or program. As specified in DOC CTR-019: *Risk Management Framework*, the ISSO must be identified on the list of key system stakeholders that is included in the required artifacts for initial system authorization.

The ISSO also serves as the principal advisor to the OU CIO, OU CISO/SAISO/ITSO, and SO on all security matters for the information system. In close coordination with the SO, the ISSO often plays an active role in developing and updating the SSP as well as in managing and controlling changes to the system and assessing the security impact of those changes. The ISSO also completes the DOC IT Compliance in Acquisition Checklist or a materially similar checklist in coordination with the following individuals, as appropriate: Cognizant OCIO, Cognizant OCIO Representative, OU Contracting Officer's Technical Representative (COTR), OU-approved Program/Requesting Office, ITSO, and Contracting Officer (CO).

3.3.12 Security Controls Assessor (SCA)

The SCA is responsible for conducting a comprehensive security assessment of the security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The SCA also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security assessment activities that are a part of the assessment and authorization process, the SCA provides an independent assessment of the SSP to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements.

3.3.13 Additional Roles

The Department defines the following additional roles, and delegates responsibilities to the individuals possessing these roles:

3.3.13.1 Contracting Officer (CO)

The COs are responsible for managing contracts/acquisitions. This includes overseeing their implementation, working in partnership with the CISO/SAISO to ensure that contracting policies adequately address the information and technology security requirements, and collaborating with the COTRs to monitor contract performance for compliance with DOC, OU, and application specific information security policies.

COs must ensure that:

- The DOC IT Compliance in Acquisition Checklist or a materially similar checklist is followed for new contracts within their responsibility; and
- Any security clauses are developed and used in accordance with Departmental procurement policy, the Commerce Acquisition Regulation (CAR) and Federal Acquisition Regulation (FAR).

3.3.13.2 Contracting Officer's Technical Representative (COTR)

The COTRs, also known as CORs, are responsible for collaborating with the COs in evaluating the need for access to DOC information and/or technological resources, ensuring appropriate background investigation clearances prior to access, and monitoring such access throughout the contract term.

Specifically, the COTRs/CORs must:

- Ensure foreign nationals will only be granted access to or perform duties on IT systems in accordance with the DOC Manual of Security Policies and Procedures and DAO 207-12;
- Notify SOs of new users and notify them to revoke access privileges in a timely manner when a user under their supervision or oversight no longer requires access privileges or he/she fails to comply with this policy;
- Authorize remote access privileges for personnel and review remote access user security agreements on an annual basis to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (e.g., systems authorized for access, and type and version of anti-virus software and personal firewall); and
- Complete the DOC IT Compliance in Acquisition Checklist or a materially similar checklist in coordination with the following individuals, as appropriate: Cognizant OCIO, Cognizant OCIO Representative, OU ITSO, OU ISSO, OU-approved Program/Requesting Office IT Security Officer, and CO.

3.3.13.3 Supervisor

The responsibilities of a Supervisor encompass the management of subordinate users, which includes assessing, authorizing, and managing the need for access to the DOC information and/or technological resources, and taking immediate action if misuse is suspected or confirmed as defined under user responsibilities and OU and/or application specific agreements.

Specifically, Supervisors must:

- Ensure foreign nationals will only be granted access to or perform duties on IT systems in accordance with the DOC Manual of Security Policies and Procedures and DAO 207-12, *Foreign National Visitor and Guest Access Program*;
- Notify SOs of new users and notify them to revoke access privileges in a timely manner when a user under their supervision or oversight no longer requires access privileges or he/she fails to comply with this policy; and
- Authorize remote access privileges for personnel and review remote access user security agreements on an annual basis to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (e.g., systems authorized for access, and type and version of anti-virus software and personal firewall).

3.3.13.4 Account, Application, Database, Network and System Administrators

Account, Application, Database, Network and System Administrators, under the Supervisor/SO direction and specifications, are responsible for implementing IT security controls, OU-specific and application-specific policies, which minimally includes involvement of Developers and Programmers for routine testing.

3.3.13.5 Developers and Programmers

Developers and Programmers must implement IT security controls in systems and system components (including software) as specified by the Supervisor/SO to ensure compliance with IT security controls, OU-specific, and application-specific policies. This minimally includes involvement with User Representatives and in system A&A activities, such as documentation of new system components and vulnerability testing, as well as adhering to change management guidelines. Developers and Programmers shall apply information system security engineering principles in the specification, design, development, implementation, and modification of software.

3.3.13.6 Key Contingency Roles

Key contingency roles, such as those defined in COOP, Disaster Recovery, and IT Contingency Plans, have responsibilities to ensure that the respective plan is maintained, tested, integrated with other plans, is adequate in scope, and is relevant.

3.3.13.7 IT Security Incident Response Personnel

The IT Security Incident Response Personnel responsibilities include analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, coordinating incident response activities, interacting with the DOC Federation of Computer Incident Response Teams (FedCIRTs) and others to disseminate reasoned and actionable cyber security information as necessary. These responsibilities include assuring that coordination with the US-CERT and appropriate authorities occurs as necessary.

3.3.13.8 Users

Users are defined as individuals having non-public access to DOC information and/or technological resources. This scope includes those who may only have physical access within DOC facilities, or those who may only have access to shared technological resources.

All users must read, understand, and acknowledge understanding of OU and applicable application-specific policies. At a minimum, users must:

- Complete IT Security refresher training annually;
- Understand OU property (or assets) for which they are responsible (i.e., printer, desktop, etc.);
- Know the type of information handled, and understand measures to protect it;
- Understand and be proactive in management of Federal electronic records, which extends to assurance of appropriate backups of user data;
- Cooperate with designated personnel during the investigation of incidents, compliance reviews, audits, and/or surveys regarding the security posture of the OU;
- Report suspected or confirmed security incidents (e.g., loss of Personally Identifiable Information (PII), virus or malicious code attacks) as procedurally defined by the OU;
- Obey copyrights and do not download, install, or access Peer-to-Peer (P2P) file sharing software;
- Understand only SO-approved individuals are allowed to download and install OU-approved applications onto DOC IT resources;
- Understand the consequences of actions of misuse;
- Understand that all use and content of IT systems, including computers, may be monitored, and reviewed for security purposes, as per CINTR-022: *Access and Use Policy*; and
- Sign appropriate access agreements prior to being granted access.

3.4 DOC IT Groups

The following forums have been established to ensure continuous collaboration at multiple levels. Depending on the current DOC security posture, environment, or architecture, other forums and/or groups are established to address or review a specific issue or subject area.

3.4.1 CIO Council

As defined in DOO 15-23, *Chief Information Officer*, the CIO Council promotes effective IT management practices throughout the Department and shares information of a crosscutting nature, and is chaired by the DOC CIO.

3.4.2 Commerce IT Review Board (CITRB)

As defined in DOO 15-23, *Chief Information Officer*, the Commerce Information Technology Review Board (CITRB), chaired by the DOC CIO, reviews and evaluates proposed IT initiatives and requests for acquisitions, reviews and evaluates ongoing IT projects, and guides a capital asset management process.

3.4.3 Enterprise Architecture (EA) Advisory Group

The EA Advisory Group serves as a Department-wide forum for definition of a blueprint that explains how the results of strategic planning, performance planning, budgeting, capital planning and investment control, security and privacy, acquisition, and other related IT and general management processes work together to meet the enterprise's mission and objectives. The group defines the future state of DOC's IT based on business and technology drivers as well as the transition plan for moving from the current state to the future.

3.4.4 IT Security Coordinating Committee (ITSCC)

The ITSCC serves as a Department-wide forum for sharing information addressing issues and making recommendations related to IT security responsibilities and activities that affect the DOC as a whole. The ITSCC is subordinate to and reports to the CIO Council, and is sponsored by the DOC CIO. The DOC CISO facilitates the ITSCC.

3.4.5 Web Advisory Council (WAC)

The Department of Commerce Web Advisory Council (WAC) was established to support the management of the Department's Web sites, to achieve compliance with applicable laws, regulations, and OMB directives, and to support high quality information services to the public.

The WAC develops policies to aid in the implementation of applicable laws, regulations, and directives and provides recommendations to the Department of Commerce Chief Information Officer (DOC CIO) and the Department of Commerce CIO Council on Web-related matters.

3.4.6 Electronic and IT (EIT) Accessibility Coordinator and Commerce Information Quality Task Force

The EIT Accessibility Coordinator disseminates information on EIT accessibility matters to the OUs and facilitates cooperation among them on accessibility issues.

The Information Quality Act mandates the issuance of information quality guidelines. This legislation affords Commerce the opportunity to highlight its commitment to information quality

by posting its information quality and peer review guidelines to demonstrate a thorough and professional approach to information release. The Commerce Information Quality Task Force is the Office of the Secretary (OS) and OU Staff that coordinates the implementation of the Act and communicates implementation status to OMB.

3.4.7 Federation of Computer Incident Response Teams (FedCIRTs)

For each bureau operating within Commerce, that has an established Computer Incident Response Team (CIRT) that provides incident response for their respective bureau. The remaining Commerce bureaus receive cyber incident response support from the centrally managed DOC FedCIRTs.

To support this decentralized computer incident response capability, Commerce also manages the FedCIRTs - where all CIRTs within the Department are represented. This intra-Departmental forum allows all Commerce CIRTs to share information on a particular incident, discuss technology and security countermeasures, and leverage Department-wide resources in the event of a large-scale attack.

3.4.8 Commerce Capital Planning and Investment Control (CPIC) Community

The CPIC Community performs reviews of proposed IT initiatives and projects in the development phase and conducts monthly assessments of all major IT investments. In addition, the CPIC process supports TechStat reviews, periodic review by the Commerce IT Review Board and stage gate reviews by the Executive level management review board of significant on-going IT projects and systems currently in operation. These reviews support the systematic analysis and adjustment of the OS IT portfolio.

3.4.9 HSPD-12 Working Group

The HSPD-12 Working group provides a forum for discussing issues, defining and resolving technical problems, recommending solutions concerning, and developing policy related to HSPD-12 implementation throughout the Department and its OUs.

3.4.10 IT Audit Working Group

The IT Audit Working Group is a joint effort between Office of Financial Management (OFM) and OCIO to manage and remediate findings from the Financial Statements IT Audit and to develop enterprise wide solutions.

3.4.11 DOC Privacy Council

The DOC Privacy Council works to strengthen Department privacy policies to ensure that they reflect the goals, values, and policies that the Department advocates. The Council Chair, Vice Chair, and Executive Committee fulfill the role of the Senior Agency Official for Privacy (SAOP). The SAOP has overall responsibility and accountability for ensuring the Department's implementation of information privacy protections, including the Department's full compliance with federal laws, regulations, and policies relating to information privacy.

3.4.12 DOC PII Breach Response Task Force

The DOC PII Breach Response Task Force is the core management team responsible for providing in-depth analysis and recommendations for an appropriate response to PII breaches that may cause significant harm to individuals or the Department.

3.5 DOC Offices

Given the reliance on and use of information technology, all DOC offices must coordinate, particularly with the OCIO. This includes, but is not limited to, the following department-level offices: CFO/Assistant Secretary for Administration, Office of General Counsel (OGC), Office of Inspector General (OIG), Office of Legislative and Intergovernmental Affairs (OLIA), Office of Policy and Strategic Planning (OPSP), and Office of Public Affairs (OPA). These offices may also coordinate with OU-equivalent offices to ensure consistency in the sharing and application of security policies and procedures.

3.5.1 Office of the Chief Information Officer (OCIO)

As defined in DOO 15-23, the OCIO is responsible for implementing the Clinger-Cohen Act of 1996, leading the management of information resources throughout the Department, and ensuring that the Department's programs make full and appropriate use of information technology.

3.5.2 Office of Cyber Security (OCS)

As defined in DOO 15-23, *Chief Information Officer*, the OCS must direct and implement a Department-wide cyber security program, which includes:

- The development and implementation of a Department-wide risk management strategy to assess, respond to and monitor Department cyber security risk at the organizational level, mission/business process level and information system level; and
- The implementation of a cyber security risk management framework that guides operating units in the security categorization of information systems, selection of security controls, authorization of information systems, and the continuous monitoring of information systems and IT assets.

OCS monitors Federal IT security laws, regulations, policies, and guidance to develop Department-level security policies. It also conducts ongoing security compliance reviews and assessments, develops performance metrics, and publishes scorecards assessing the effectiveness of OU security programs. It maintains Department-wide Plans of Action and Milestones (POA&Ms) to record weaknesses and monitor remediation. It directs the Department's Enterprise Cyber Security Program, which focuses on effectively and efficiently implementing Department-wide IT security initiatives. It directs the Department's National Security and Critical Infrastructure Protection Program. Lastly, OCS maintains a Department-wide information security awareness and training program that establishes OU security training requirements and monitors compliance with these requirements.

3.5.3 Office of Security (OSY)

OSY is responsible for identifying, assessing, and managing mission-critical threats and providing guidance regarding the physical and environmental security controls that protect the DOC's information system assets. Facility security policies are established and promulgated by this office. These controls include ensuring the COOP development and continuity of government programs, security clearance management, and physical access control mechanisms, among others, are established.

The OSY is responsible for managing the Department's security programs, including those in the area of:

- Physical security of facilities and equipment external to computers or telecommunication lines;
- Protection of national security information;
- Personnel security, including performance of background checks and security clearance investigations of personnel;
- Coordinating with the DOC CIPM on the physical security aspect of critical infrastructure protection;
- Emergency planning; and
- Conducting investigations to identify and/or assess threats to the Department's mission, operations, or activities and protect Department personnel, facilities, property, or assets including IT-related incidents with a counterintelligence, criminal intelligence, protective intelligence, or counterterrorism nexus.

Further information regarding responsibilities of OSY, Operating Unit Heads, and Departmental facility/office managers is available in the DOC Manual of Security Policies and Procedures (Chapters 1 and 2), and the appropriate Departmental directives and orders (i.e., the DAO 207 series, Security and Loyalty, as well as DOO 20-6, *Director for Security*).

3.5.4 Office of Acquisition Management (OAM)

The Office of Acquisition Management (OAM) administers and oversees the Department of Commerce (DOC) acquisition function through delegated procurement authority provided to five operating units: National Oceanic and Atmospheric Administration (NOAA), National Institute of Standards and Technology (NIST), Patent and Trademark Office (PTO), Census Bureau, and the Office of the Secretary (OS). OAM also maintains an operational acquisition division, Commerce Acquisition Solutions (CAS), which provides operational acquisition support to the Office of the Secretary. The Director of OAM serves as the Senior Procurement Executive (SPE) for the Department. The SPE has overall responsibility for planning, developing, and implementing policies and procedures for acquisitions for DOC; overseeing the acquisition planning process through oversight reviews of procurement offices; and participating on Bureau and DOC Acquisition Review Boards for larger acquisitions or acquisitions of special interest to DOC.

Senior Bureau Procurement Officials (BPO) are the senior career procurement officials within each of five operating units with delegated contracting authority. Heads of Contracting Office (HCO) are designated by the senior BPO to head a contracting office within each operating unit with contracting authority. Contracting Officers (CO) are warranted individuals with designated authority to enter into, administer, and/or terminate contracts and make related determinations and findings. Contracting Officer Representatives (COR), Assistant or Alternate Contracting Officer Representatives (ACOR) and Task Managers (TM), are CO Representatives with delegated authority to monitor and provide specific contract management duties under a contract. Program/Project Managers direct a group of related activities performed within a specified time period to meet a specific set of objectives.

The OAM public website is located at <http://www.osc.doc.gov/oam/> and includes acquisition policy and guidance is located at http://www.osc.doc.gov/oam/acquisition_management/policy/default.htm. Posted acquisition policy and guidance includes: acquisition-related Commerce Acquisition Directives (DOO) and Department Administrative Orders (DAO); the Federal Acquisition Regulation (FAR); the Commerce Acquisition Regulation (CAR), which implements the FAR; the Commerce Acquisition Manual (CAM); Procurement Memoranda; and various OMB Circulars and Office of Federal Procurement Policy (OFPP) Policy Letters. Congressional appropriation restrictions affecting DOC acquisitions are addressed in Procurement Memoranda.

Acquisition planning is required for all acquisitions -- especially acquisitions for information technology. Early and comprehensive acquisition planning is critical to a successful outcome and must begin *as soon as the requirement becomes known*. Primary responsibility for acquisition planning, including development of the acquisition plan, is with the program office. Early and close collaboration with the acquisition team including the contracting officer, legal counsel, information technology, security, budget/finance, small business and others, as appropriate, is essential. The extent of acquisition planning and review will vary depending on the size and nature of the acquisition.

The program official serves as the “planner” in the acquisition planning process, as defined in FAR Section 7.101. With the advice and assistance of the Contracting officer, the planner is responsible for: preparing and maintaining acquisition plans; preparing justifications for other than full and open competition; obtaining and documenting all necessary concurrences and approvals; coordinating with the acquisition team for advice and assistance; complying with the acquisition planning requirements in FAR Part 7, DAO 208-15, DOC policy and guidance in the CAR and CAM, etc.; coordinating with the Bureau Small Business Specialist and Office of Small and Disadvantaged Business Utilization (OSDBU); coordinating with operating unit (OU) representatives of the Chief Financial Officer and Budget Officer; coordinating with OU representatives of the Chief Information Officer on acquisitions requiring capital planning and investment control requirements as identified in 40 U.S.C. 11312 and OMB Circular A-130, any congressional restrictions relating to IT, and other special requirements; ensuring at least one qualified Contracting Officer’s Representative (COR) is nominated as early as practicable; continually monitoring the acquisition forecast and updating quarterly to reflect Departmental and OMB budgetary decisions and reprogramming, correction of errors, or emergency requirements; and modifying the acquisition plan for major changes, both before and after contract award, and obtaining new coordination, concurrences, and approval.

The acquisition of IT is subject to many federal and DOC requirements and clearances. When

acquiring IT, the program office (customer) is responsible for early and close coordination with the bureau level OCIO, acquisition, security, budget, and others offices as necessary to be sure requirements are addressed. CAR 1339.107-70, Information Security, requires the preparation of the DOC IT Compliance in Acquisitions Checklist or a materially similar checklist for IT service acquisitions over the micro-purchase threshold. Recent Congressional appropriation restrictions impose additional requirements on the acquisition of certain DOC IT.

The contracting officer, working with the acquisition team, assists the program office to ensure IT security is addressed at all stages of the acquisition (i.e., from the earliest stages of budgeting, through acquisition planning, requirements development, solicitation, source evaluation and selection, contract award and administration). The contracting officer is responsible for addressing IT security in solicitations and contracts by inserting applicable FAR and DOC clauses (such as those in CAM 1337.70, Personnel Security Processing for contractors performing services on or within a Department of Commerce facility or through an IT system, as set forth in the DOC Manual of Security Policies and Procedures and the DOC ITSPP --which address risk and sensitivity levels, background investigations and security processing requirements; Foreign Nationals; and contract requirements and procedures).

3.5.5 Office of Human Resources Management (OHRM)

The Office of Human Resources Management (OHRM) maintains the Service Level Agreement (SLA) between the National Finance Center (NFC) and DOC. The SLA is for the NFC to provide payroll services for DOC. In addition, the NFC database may be used to document the status of personnel access to information resources (e.g., employment status). The NFC database is a resource used in conjunction with OSY resources to maintain the status of position designations (Risk/Sensitivity). Position designation drives suitability/security background investigation and reinvestigation requirements. This database consists of Privacy Act (PA) information, which must be maintained consistent with PA requirements and can only be disclosed pursuant to disclosure provisions of the PA.

Servicing Human Resources Offices (SHROs) manage the human resources records for all of their respective Operating Unit (OU) personnel. The responsibilities of the SHROs for the maintenance of security of IT resources include:

- Providing timely and accurate information concerning personnel hiring, transfer, and termination to the OU CISO/SAISO/ITSO;
- Assisting in the administration of IT Security Awareness training for new employees in accordance with the DOC Manual of Security Policies and Procedures, Chapter 3;
- Maintaining records concerning personnel security violations if resulting in disciplinary action;
- Maintaining position descriptions for all positions within serviced area;
- Developing and providing guidance on procedures for disciplinary and/or adverse action due to IT security violations; and
- Maintaining personnel records containing the status of background checks and investigations of all personnel in accordance with the DOC Manual of Security Policies and Procedures, Chapter 11.

3.5.6 Office of Inspector General (OIG)

The OIG provides independent oversight through audit and evaluation of the Department's IT Security Program, in accordance with the Inspector General Act of 1978 (Public Law 95-452). In this capacity, the OIG conducts audits of financial system controls, and evaluates the Department's compliance with FISMA requirements. The OIG also assists in the investigation of computer incidents that require coordination with external law enforcement agencies. Policies relating to these areas can be found in appropriate Departmental directives, e.g., DAO 207-10, *Inspector General Investigations*.

Each OU CIO or OU CISO/SAISO/ITSO must maintain cooperative relationships with the OIG, including specific agreements and procedures covering incident response and forensics investigations if applicable. Incidents involving suspected fraud, waste, or abuse of government resources must be reported to the OIG Fraud Hotline for investigation.

3.5.7 Office of General Counsel (OGC)

The OGC reviews all policy, IT security requirements, MOUs, and contract security clauses to ensure compliance with all applicable laws and regulations.

OGC helps by reviewing DOC IT security policies to ensure the policies are aligned with current legal requirements. OGC also reviews the legality of IT security contract clauses used by OAM in DOC contracts.

3.5.8 Office of Privacy and Open Government (OPOG)

The Office of Privacy and Open Government is responsible for the development and maintenance of privacy policies, procedures, and guidance essential to safeguarding the collection, access, use, dissemination, and storage of personally identifiable information (PII) and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), and policy and guidance issued by the President and Office of Management and Budget (OMB).

4 Baseline Security Controls

Baseline controls defined in NIST SP 800-53 Rev. 4 must be employed based on the FIPS 199 security categorization of the information system. OUs must ensure that proper security controls are in place based on the impact level, risk environment and needs of the information system. These may include security controls that were not specifically listed in the catalog below. OUs must refer to NIST SP 800-53 Rev. 4 for those controls that are not included in the ITSPP but are required for baselines applicable to their systems. OUs may supplement the DOC ITSPP minimum requirements with more stringent requirements justified by a risk-based management decision to require additional controls within the OU-defined environment.

The DOC ITSPP adheres to the following principles:

- Security controls that require no additional details necessary for implementation have not been repeated from NIST SP 800-53 Rev. 4. Security controls that do not require defined parameters have not been repeated from 800-53r4. Additionally, security controls that must be defined at the OU or system-level are not included. OUs must refer to NIST SP 800-53r4 for implementation details for these controls;
- Security controls that require DOC-specific parameters and/or criteria are defined below;
- OUs must consider DOC criteria for a control as additions to or elaboration of the supplemental guidance provided in NIST SP 800-53 Rev. 4. DOC Criteria have been mapped to the baselines to which they apply. OUs must use the supplemental guidance as well as DOC criteria when implementing controls;
- Relevant DOC CITRs, policy memoranda, and FAQs are cited or referenced but not integrated into policy statements. All current DOC CITRs, Policy Memoranda, and FAQs will continue to be effective until otherwise directed;
- Security controls and control enhancements that are not selected in NIST SP 800-53 Rev. 4 for Low, Moderate or High baselines will not be required and are not included in the DOC ITSPP unless deemed necessary for inclusion;
- Parameters determined to be feasible for implementation enterprise-wide have been defined at the DOC-level and described herein; and
- Parameters for which it is not feasible to define a minimum requirement at the DOC/enterprise level (due to scope issues and/or differing architectural environments) are to be defined at the OU or system level. The parameters that are to be OU- or system-level defined are not listed in the security control catalog below.

4.1 Security Control Policies and Procedures

For all security control families, the DOC requires OUs to:

- a. Develop, document, and disseminate to **all government and contractor personnel with IT security responsibilities in the system development life-cycle:**
 1. A policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the policy and associated security controls; and
- b. Review policies and procedures **at least annually** and update **as needed**.

4.2 Security Control Catalog Key

Control Number – Security controls will be listed as follows: Control Family Abbreviation – Control Number. Enhancement Number. For example: AC-2.1 refers to Access Control, Control Number 2, Enhancement Number 1.

Control Name/Requirement – Lists the title of the control/enhancement and details necessary for implementation.

Security Baselines – Baselines (Low, Moderate, or High) selected as applicable by NIST SP 800-53 Rev. 4 will be noted for each control.

4.3 Access Control (AC)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Account Management				
AC-2	<p>Account Management</p> <p>The DOC requires the OUs to manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.</p> <p>The DOC requires the OUs to review accounts for compliance with account management requirements at least annually.</p> <p><i>Refer to DOC Account Deactivation Timeframe Policy Reminder Memo (May 20, 2013).</i></p>	X	X	X
AC-2.2	<p>Removal of Temporary/Emergency Accounts</p> <p>The DOC requires the OUs to ensure that information systems automatically remove and/or disable temporary and emergency accounts not more than 30 days after they are created.</p>		X	X
AC-2.3	<p>Disable Inactive Accounts</p> <p>The information system automatically removes and/or disables inactive accounts after 30 days. The access period for temporary/emergency accounts must not</p>		X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	exceed 30 days.			
Separation of Duties				
AC-5	Separation of Duties The DOC requires OUs to ensure that information systems enforce separation of duties through assigned access authorizations. The following three (3) categories of “duty”, at a minimum, shall be kept separate or compensating controls put in place to monitor activity closely: <ol style="list-style-type: none"> 1. IT administration or operation (assuring systems function, to serve the system users); 2. IT security: Operational, Oversight/Policy, and Auditing (assuring adequacy of system controls for availability, integrity, and confidentiality); and, 3. IT management (allocating adequate resources for implementation of effective IT Security Programs and system controls). Due to staffing constraints, the System Owner may authorize the use of dual roles (e.g., a System Administrator may serve as a back-up for an ISSO who is on leave). However, while serving in a dual role, compensating management controls must be implemented to ensure changes to the security posture are properly authorized.			
			X	X
Unsuccessful Login Attempts				
AC-7	Unsuccessful Login Attempts The DOC requires the OUs to ensure that information systems enforce a maximum of five (5) consecutive invalid access attempts by a user during a fifteen (15) minute period . The information system automatically locks the account/node for a minimum of fifteen (15) minutes or delays next login prompt according to a specified organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded. DOC Criteria: Locked accounts with privileged access (i.e., root or administrator access) will remain locked until unlocked by the respective Help Desk, Security Administrator, or other authorized account management personnel.			
		X	X	X
System Use Notification				

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
AC-8	System Use Notification The DOC requires the OUs to ensure that information systems display an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.			
	DOC Criteria: The DOC requires the following text be inserted in the message in order to give users proper notification: "You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all computers connected to this network, and 4) all devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; you have no reasonable expectation of privacy regarding any communication of data transiting or stored on this information system; at any time and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose."	X	X	X
Session Lock				
AC-11	Session Lock The DOC requires the OUs to ensure that information systems prevent further access to the system by initiating a session lock after thirty (30) minutes of inactivity , and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.		X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	<p>DOC Criteria: The DOC requires OUs to initiate session lock after thirty (30) minutes of inactivity for web applications, remote access, and portable devices, and fifteen (15) minutes of inactivity for desktop systems. For all other session locks (application or system specific), the time period must be defined by the OU.</p> <p>“Inactivity” is defined as only those actions that require interaction of a user (i.e., system and application calls are not included).</p>			
Session Termination				
AC-12	<p>Session Termination</p> <p>The DOC requires the OUs to ensure that information systems automatically terminate a remote session after thirty (30) minutes of inactivity.</p> <p>DOC Criteria: “Inactivity” is defined as only those actions that require interaction of a user (i.e., system and application calls are not included).</p>		X	X
Remote Access				
AC-17	<p>Remote Access</p> <p><i>Refer to CTR-008: Remote Access and CTR-20: Safeguarding Information While on Foreign Travel for control details.</i></p>	X	X	X
AC-17.2	<p>Protection of Confidentiality/Integrity Using Encryption</p> <p><i>Refer to CTR-008: Remote Access and CTR-20: Safeguarding Information While on Foreign Travel for control details.</i></p>		X	X
Wireless Access				
AC-18	<p>Wireless Access</p> <p><i>Refer to CTR-014: Wireless Encryption Enhancements Policy for control details.</i></p>	X	X	X
Access Control for Mobile Devices				
AC-19	<p>Access Control for Mobile Devices</p> <p><i>Refer to CTR-008: Remote Access and CTR-020: Safeguarding Information While on Foreign Travel for control details.</i></p>	X	X	X
Use of External Information Systems				
AC-20	<p>Use of External Information Systems</p> <p><i>Refer to NIST SP 800-53 Rev. 4 AC-20 for control details.</i></p>	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	DOC Criteria: The DOC requires the OUs to verify and document requirements in an Interconnection Security Agreement (ISA), Memorandum of Agreement (MOA), Memorandum of Understanding (MOU) and/or contract.			
AC-20.2	Portable Storage Devices The DOC restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.		X	X

4.4 Security Awareness and Training (AT)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Security Awareness Training				
AT-2	Security Awareness Training The DOC requires the OUs to provide basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter based on fiscal year. DOC Criteria: A user may be granted temporary access where an information system security orientation is provided with granted access, until the training requirement can be met. In this instance, training shall be met within thirty (30) calendar days. If a user refuses to engage in, or cannot meet the training requirement due to extenuating circumstances, access to information and resources must be suspended, and a risk-based decision whether to reinstate access made by the AO.	X	X	X
Role-Based Security Training				
AT-3	Role-Based Security Training <i>Refer to CITR-006: Information System Security Training for Significant Roles for control details.</i>	X	X	X
Security Training Records				
AT-4	Security Training Records <i>Refer to CITR-006: Information System Security Training for Significant Roles for control details.</i>	X	X	X

4.5 Audit and Accountability (AU)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Audit Events				
AU-2	Audit Events The DOC requires the OUs to ensure the information system generates audit records for events as defined by the OU. DOC Criteria: The list of auditable events to be recorded should include, but is not limited to: account logon events, account management events, directory service access events, object access failures, policy change failures, privilege use failures, and system events. Other events must be defined by the OU. The DOC requires logging all computer-readable data extracts from databases holding sensitive information (refer to OMB M-06-16: Protection of Sensitive Agency Information).	X	X	X
AU-2.3	Reviews and Updates The DOC requires the OUs to review and update list of audited events at least annually .		X	X
Content of Audit Records				
AU-3	Content of Audit Records <i>Refer to NIST SP 800-53 Rev. 4 AU-3 for control details.</i> DOC Criteria: The DOC requires the following record content for data extracts from databases holding sensitive information: date of extraction, date of extraction deletion, name of extractor, and storage location of extraction.	X	X	X
AU-3.2	Centralized Management of Planned Audit Record Content The DOC requires the OUs to ensure the information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.			X
Response to Audit Processing Failures				
AU-5.1	Audit Storage Capacity The DOC requires the OUs to ensure the information system provides a warning when allocated audit record storage volume reaches 90% of maximum audit record			X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	storage capacity.			
AU-5.2	Real-Time Alerts The DOC requires the OUs to ensure the information system provides a real time alert when the following audit failure events occur: software/hardware error, failure in audit capturing mechanism, and capacity met for audit record storage capacity.			X
Time Stamps				
AU-8	Time Stamps DOC requires information systems to: <ol style="list-style-type: none"> Use internal system clocks to generate time stamps for audit records; and Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and are accurate to the second. 	X	X	X
Audit Record Retention				
AU-11	Audit Record Retention The DOC requires the OUs to retain audit logs for at least ninety (90) days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	X	X	X
Audit Generation				
AU-12.1	Time-Correlated Audit Trail DOC information systems must compile audit records from events listed in AU-2 into a system-wide (logical or physical) audit trail that is time-correlated to within 2 seconds .			X

4.6 Security Assessment and Authorization (CA)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Security Assessments				
CA-2	Security Assessments Refer to CITR-019: Risk Management Framework (RMF) for control details.	X	X	X
CA-2.2	Specialized Assessments Refer to CITR-019: Risk Management Framework (RMF) for control details.			X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Information and System Connections				
CA-3	Information and System Connections <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i> DOC Criteria: The DOC requires OUs to review and update Interconnection Security Agreements at least annually and update as necessary.	X	X	X
Plan of Action and Milestones				
CA-5	Plan of Action and Milestones <i>Refer to CITR-018: IT Security Plans of Action and Milestones (POA&M) for control details.</i>	X	X	X
Security Authorization				
CA-6	Security Authorization <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i>	X	X	X
Continuous Monitoring				
CA-7	Continuous Monitoring <i>Refer to OMB M-14-03: Enhancing the Security of Federal Information and Information Systems and CITR-019: Risk Management Framework (RMF) for control details.</i>	X	X	X
CA-7.1	Independent Assessment <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i>		X	X
Penetration Testing				
CA-8	Penetration Testing Penetration testing must be conducted at least annually as part of annual assessment.			X

4.7 Configuration Management (CM)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Baseline Configuration				
CM-2.1	Reviews and Updates			
	<i>Refer to CITR-017: Security Configuration Checklist Program for control details.</i>			
	Baseline configuration documentation must be reviewed and updated:			
	a. At least annually;			

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	b. When required due to a significant system change; and c. As an integral part of information system component installations and updates.			
CM-2.3	Retention of Previous Configurations The DOC requires OUs to retain at minimum one previous version of the system configuration to support rollback.		X	X
CM-2.4	Configure Systems, Components, or Devices for High-Risk Areas <i>Refer to CITR-20: Safeguarding Information While on Foreign Travel for control details.</i>		X	X
Security Impact Analysis				
CM-4	Security Impact Analysis <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i>	X	X	X
CM-4.1	Separate Test Environments <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i>			X
Configuration Settings				
CM-6	Configuration Settings <i>Refer to CITR-017: Security Configuration Checklist Program for control details.</i>	X	X	X
Least Functionality				
CM-7.1	Periodic Review <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i>		X	X
CM-7.2	Prevent Program Execution The list of prohibited and/or restricted functions, ports, protocols, and/or services, shall be included in the SSP.		X	X
Information System Component Inventory				
CM-8	Information System Component Inventory <i>Refer to CITR-017: Security Configuration Checklist Program for control details.</i>	X	X	X
CM-8.3 E(3)	Automated Unauthorized Component Detection <i>Refer to CITR-017: Security Configuration Checklist Program for control details.</i> The DOC requires OUs to take action as appropriate to address detection of unauthorized components.		X	X
Software Usage Restrictions				

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
CM-10	Software Usage Restrictions			
	<i>Refer to CITR-011, Peer-to-Peer Technology and CITR-022: Access and Use for control details.</i>	X	X	X
User-Installed Software				
CM-11	User-Installed Software			
	<i>Refer to CITR-022: Access and Use, for control details.</i>	X	X	X

4.8 Contingency Planning (CP)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Contingency Plan				
CP-2	Contingency Plan The DOC requires the OUs to develop and implement a Contingency Plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the Contingency Plan and distribute copies of the plan to key contingency personnel at least annually and update as needed.	X	X	X
CP-2.3	Resume Essential Missions/Business Functions <i>See OMB M-04-15: Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources</i> <i>for related requirements.</i>		X	X
CP-2.8	Identify Critical Assets <i>See OMB M-04-15: Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources</i> <i>for related requirements.</i>		X	X
Contingency Training				
CP-3	Contingency Training <i>Refer to CITR-006: Information System Security Training for Significant Roles</i> <i>for control details.</i>	X	X	X
CP-3.1	Simulated Events <i>Refer to CITR-006: Information System Security Training for Significant Roles</i> <i>and CITR-015: Contingency Plan Testing and Exercise Activities</i> <i>for</i>			X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	<i>control details.</i>			
Contingency Plan Testing and Exercise				
CP-4	Contingency Plan Testing <i>Refer to CITS-015: Contingency Plan Testing and Exercise Activities and FAQ II for control details.</i>	X	X	X
CP-4.2	Alternate Processing Site <i>Refer to CITS-015: Contingency Plan Testing and Exercise Activities for control details.</i>			X
Telecommunications Services				
CP-8	Telecommunications Services <i>Refer to OMB M-05-16: Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings for control details.</i>		X	X
Information System Backup				
CP-9.1	Testing for Reliability/Integrity The DOC requires the OUs to test backup information at least annually to verify media reliability and information integrity. <i>Refer to CITS-015: Contingency Plan Testing and Exercise Activities and FAQ II for control details.</i>		X	X
CP-9.3	Separate Storage For Critical Information The DOC requires the OUs to store backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.			X
Information System Recovery and Reconstitution				
CP-10	Information System Recovery and Reconstitution The DOC requires the most recent secure backups for system components should include the most recent known baseline configuration for all components.	X	X	X

4.9 Identification and Authentication (IA)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
User Identification and Authentication				
IA-2	Identification and Authentication (Organizational Users) The DOC requires the OUs to ensure the information system uniquely identifies and authenticates users (or	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	<p>processes acting on behalf of users).</p> <p>DOC Criteria: For remote access, DOC requires two-factor authentication (Level 3 compliant as defined in CITR-008: <i>Remote Access</i>) where one factor is provided by a device separate from the computer gaining access for remote access. See OMB M-04-04, <i>E-Authentication Guidance for Federal Agencies</i>, OMB M-06-16, <i>Protection of Sensitive Agency Information</i>, OMB M-06-19, <i>Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments</i>, and OMB M-07-16, <i>Safeguarding Against and Responding to the Breach of Personally Identifiable Information</i>.</p> <p>For remote access by portable and mobile devices, DOC requires the use of two-factor authentication where one factor is provided by a device separate from the computer gaining access.</p> <p><i>Refer to Policy Memorandum for the Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12) for control details.</i></p>			
Authenticator Management				
IA-5.1	<p>Password-Based Authentication</p> <p><i>Refer to CITR-021: Password Management for control details.</i></p>	X	X	X
IA-5.11	<p>Hardware Token-Based Authentication</p> <p><i>Refer to M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors for control details.</i></p>	X	X	X

4.10 Incident Response (IR)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Incident Response Training				
IR-2	Incident Response Training <i>Refer to CITR-006: Information System Security Training for Significant Roles for control details.</i>	X	X	X
Incident Response Testing				

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
IR-3	Incident Response Testing The DOC requires the OUs to test the incident response capability for the information system at least annually using OU-defined tests to determine the incident response effectiveness and documents the results. Responding to a genuine security incident will fulfill the annual testing requirement.		X	X
Incident Monitoring				
IR-5	Incident Monitoring The DOC requires the OUs to track and document information system security incidents on an ongoing basis .	X	X	X
Incident Reporting				
IR-6	Incident Reporting The DOC requires the OUs to: a. Require personnel to report suspected security incidents and PII breaches to the organizational incident response capability as soon as possible. The organizational incident response capability must report the PII incident to the DOC Chief Privacy Officer, DOC-CIRT (where DOC-CIRT is not the receiving CIRT), and US-CERT within one (1) hour of discovery/detection; and b. Report security incident information to the servicing incident response team.	X	X	X
Incident Response Assistance				
IR-7	Incident Response Assistance The DOC requires the OUs to provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the DOC incident response capability.			
	DOC Criteria: The US-CERT provides assistance to the DOC FedCIRT in handling incidents, technical inquiries, as well as alerts and advisories, via a 24-hour Incident Response Center. User assistance must be provided as part of each OU's Incident Response capability. The OSY Investigations and Intelligence Program provides assistance to the DOC FedCIRT in handling incidents, technical inquiries, as well as alerts and	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	advisories that have a counterintelligence nexus.			

4.11 Media Protection (MP)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Media Labeling				
MP-3	Media Marking The DOC requires the OUs to: (i) affix external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempt specific types of OU-defined media or hardware components from labeling so long as they remain within the OU-defined protected environment.		X	X
Media Transport				
MP-5	Media Transport The DOC requires the OUs to: a. Protect and control removable media devices as required by CITR-005: <i>Removable Media Devices</i> ; b. Maintain accountability for information system media during transport outside of controlled areas; c. Document activities associated with the transport of information system media; and d. Restrict the activities associated with the transport of information system media to authorized personnel.		X	X
MP-5.4	Cryptographic Protection <i>Refer to CITR-005: Removable Media Devices and CITR-020: Safeguarding Information While on Foreign Travel for control details.</i>		X	X
Media Use				
MP-7	Media Use <i>Refer to CITR-005: Removable Media Devices for control details specific to Moderate and High systems.</i>	X	X	X

4.12 Physical and Environmental Protection (PE)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Physical Access Authorizations				
PE-2	Physical Access Authorizations	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	The DOC requires the OUs to: a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals at least annually ; and d. Remove individuals from the facility access list when access is no longer required.			
Access Control for Display Medium				
PE-5	Access Control for Output Devices The DOC requires the OUs to control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.		X	X
Monitoring Physical Access				
PE-6	Monitoring Physical Access The DOC requires the OUs to: a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Review physical access logs at least annually and upon occurrence of OU-defined events or potential indications of events; and c. Coordinate results of reviews and investigations with the organizational incident response capability.	X	X	X
Visitor Access Records				
PE-8	Visitor Access Records The DOC requires the OUs to: a. Maintain visitor access records to the facility where the information system resides for at least one year ; and b. Review visitor access records at least annually .	X	X	X

4.13 Planning (PL)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
System Security Plan				
PL-2	System Security Plan Refer to CITR-019: Risk Management Framework (RMF) for control details.	X	X	X
Rules of Behavior				
PL-4	Rules of Behavior The DOC requires the OUs to ensure written acknowledgement of CITR-022: Access and Use	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	<i>Policy and/or an OU-specific equivalent policy prior to granting access to any non-public IT systems, networks, or resources. This may be accomplished by providing employees with a copy of the policy and obtaining a written acknowledgement that they have read and understood the policy, or by developing a separate access and use form that describes this policy, to be signed by an employee or associate prior to that individual being provided access to IT systems/network/resources.</i>			
PL-4.1	Social Media And Networking Restrictions <i>Refer to CINTR-022: Access and Use Policy and the DOC Social Media Policy for control details.</i>		X	X
Information Security Architecture				
PL-8	Information Security Architecture The DOC requires the OUs to: a. Develop an information security architecture for the information system that: 1. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describe how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describe any information security assumptions about, and dependencies on, external services; b. Review the information security architecture at least annually and updates as needed to reflect updates in the enterprise architecture; and c. Ensure that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.		X	X

4.14 Personnel Security (PS)

Control Number		Control Name/Requirement	Security Baselines		
			Low	Moderate	High
Position Risk Designation					
PS-2	Position Risk Designation The DOC requires the OUs to assign a risk designation to all positions and establish screening criteria for individuals filling those positions.	X	X	X	

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	<p><i>Refer to the DOC Manual of Security Policies and Procedures §10.1 “Position Risk and Sensitivity Designation” and CAM 1337.70 for control details.</i></p> <p>DOC Criteria:</p> <p>1. OUs shall comply with the requirements of the DOC Handbook on Suitability (DAO 202-731, Position Sensitivity for Personnel Suitability and Personnel Security Purposes) and the DOC Manual of Security Policies and Procedures, which provide criteria for national security positions, and for Low, Moderate, and High “risk” non-national security positions.</p> <p>2. The CAM 1337.70, Security Processing Requirements for On-Site Service Contracts provides contract risk designation criteria and contract language for IT service contracts.</p>			
Personnel Screening				
PS-3	<p>Personnel Screening</p> <p>The DOC requires the OUs to screen individuals requiring access to organizational information and information systems before authorizing access. OUs must rescreen individuals in accordance with the DOC Manual of Security Policies and Procedures.</p> <p><i>Refer to the DOC memorandum National Security Clearance Requirement for CIOs and ITSOs (Jan. 27th, 2010) for control details.</i></p> <p>DOC Criteria: The DOC requires that all personnel be subject to an appropriate background check prior to permitting permanent access to DOC resources. Appropriate background checks must be performed on employees, contractors, and any “guests” prior to their being given long-term, permanent access to DOC information systems and networks in accordance with requirements contained in the DOC Handbook on Suitability and the DOC Manual of Security Policies and Procedures.</p>	X	X	X
Access Agreements				
PS-6	<p>Access Agreements</p> <p>The DOC requires the OUs to complete appropriate</p>	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	signed access agreements for individuals requiring access to organizational information and information systems before authorizing access, review the agreements at least annually, and update them as necessary. <i>Refer to CITR-022: Access and Use Policy for control details.</i>			
Personnel Sanctions				
PS-8	Personnel Sanctions The DOC requires the OUs to comply with the formal sanctions process established by OHRM. Violations of this policy may result in disciplinary action, up to and including dismissal and/or legal action against the offending employee(s), contractors, or visitors, consistent with applicable law and DAO 202-751, Discipline, or contract terms as applicable. <i>Refer to CITR-022: Access and Use Policy for control details.</i>	X	X	X

4.15 Risk Assessment (RA)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Security Categorization				
RA-2	Security Categorization <i>Refer to CITR-019: Risk Management Framework (RMF) and FAQ II for control details.</i>	X	X	X
Risk Assessment				
RA-3	Risk Assessment <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i>	X	X	X
Vulnerability Scanning				
RA-5	Vulnerability Scanning <i>Refer to the DOC memorandum Transmittal Memo for CITR-016 and CITR-17 (Jan. 25th, 2012) for control details.</i>	X	X	X
RA-5.1	Update Tool Capability <i>Refer to CITR-016: Vulnerability Scanning and Patch Management for control details.</i>		X	X
RA-5.2	Update by Frequency / Prior to New Scan / When Identified <i>Refer to CITR-016: Vulnerability Scanning and Patch</i>		X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	Management <i>for control details.</i>			
RA-5.3	Breadth / Depth of Coverage The DOC requires the OUs to employ vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.	X	X	X
RA-5.5	Privileged Access <i>Refer to CITR-016: Vulnerability Scanning and Patch Management for control details.</i>		X	X

4.16 System and Services Acquisition (SA)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Acquisition Process				
SA-4	<p>Acquisition Process</p> <p>The DOC requires the OUs to include security requirements and/or security specifications either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, EOs, directives, policies, regulations, and standards.</p> <p><i>Refer to the Commerce Acquisition Manual (CAM) 1337.70 for control details.</i></p> <p>DOC Criteria: The OUs utilize the DOC IT Compliance in Acquisitions Checklist or a materially similar checklist to ensure that information security is considered during the requirements definition, solicitation, and award process.</p>	X	X	X
SA-4.10	<p>Use of Approved PIV Products</p> <p><i>Refer to Policy Memorandum for the Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12) for control details.</i></p>	X	X	X
External Information System Services				
SA-9	<p>External Information System Services</p> <p>The DOC requires the OUs to:</p> <p>a. Require that providers of external information system services comply with organizational information security requirements and employ the risk management framework described in CITR-019: <i>Risk Management Framework (RMF)</i> in accordance with applicable federal laws, Executive Orders,</p>	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	<p>directives, policies, regulations, standards, and guidance;</p> <p>b. Define and document government oversight and user roles and responsibilities with regard to external information system services; and</p> <p>c. Employ OU-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.</p> <p><u>DOC Criteria:</u> The overall responsibility and accountability for securing the information and information systems remains with the DOC/OU. Therefore, the DOC requires the OUs to ensure that third-party providers of information system services employ adequate security controls in accordance with DOC ITSPP. The DOC also requires the OUs to monitor external information system security control compliance.</p>			
Developer Configuration Management				
SA-10	<p>Developer Configuration Management</p> <p>The DOC requires the OU information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.</p>		X	X
Developer Security Testing and Evaluation				
SA-11	<p>Developer Security Testing and Evaluation</p> <p>The DOC requires the OU information system developers create a security test and evaluation plan, implement the plan, and document the results.</p> <p><u>DOC Criteria:</u> Developmental security assessment results shall be used in support of the A&A process for information systems in accordance with the OU's system development life cycle.</p>		X	X
Supply Chain Protection				
SA-12	<p>Supply Chain Protection</p> <p><i>Refer to the DOC IT Compliance in Acquisitions Checklist or a materially similar checklist for control details.</i></p>			X

4.17 System and Communications Protection (SC)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Denial of Service Protection				
SC-5	Denial of Service Protection The DOC requires the OUs to ensure the information system protects against or limits the effects of the following types of Denial of Service (DoS) attacks: directed malicious attacks against DOC networks, systems, or services originating internally or from the Internet or other external networks.	X	X	X
Boundary Protection				
SC-7.3	Access Points <i>Refer to the M-08-05: Implementation of Trusted Internet Connections (TIC) and the Trusted Internet Connections (TIC) Reference Architecture Document Version 2.0 for control details.</i>		X	X
SC-7.4	External Telecommunications Services The DOC requires OUs to: (a) Implement a managed interface for each external telecommunication service; (b) Establish a traffic flow policy for each managed interface; (c) Protect the confidentiality and integrity of the information being transmitted across each interface; (d) Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Review exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need.		X	X
Network Disconnect				
SC-10	Network Disconnect The DOC requires the OUs to ensure the information system terminates a network connection at the end of a session or after thirty (30) minutes of inactivity.		X	X

4.18 System and Information Integrity (SI)

Control Number	Control Name/Requirement	Security Baselines			
		Low	Moderate	High	
Malicious Code Protection					
SI-3	Malicious Code Protection	X	X	X	

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	<p>The DOC requires OUs to:</p> <ul style="list-style-type: none"> a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Update malicious code protection mechanisms whenever new releases are available in accordance with OU configuration management policy and procedures; c. Configure malicious code protection mechanisms to: <ul style="list-style-type: none"> 1. Perform periodic scans of the information system at least monthly and real-time scans of files from external sources at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block malicious code, quarantine malicious code; send an alert to the system administrator, and/or perform some other organization-defined action(s) in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. 			
Information System Monitoring				
SI-4	<p>Information System Monitoring</p> <p>The DOC requires the OUs to protect all external access points by using network-based intrusion detection/prevention systems (IDS/IPS) and all publicly accessible DOC servers by using host-based IDSs.</p>	X	X	X
SI-4.5	<p>System-Generated Alerts</p> <p>The DOC requires the OUs to ensure the information systems provide a real-time alert when the following indications of compromise or potential compromise occur: OU-defined list of compromise indicators or indications that the system's integrity has been breached.</p>		X	X
Security Function Verification				
SI-6	<p>Security Function Verification</p> <p>The DOC requires the OUs to ensure the information system verifies the correct operation of security functions upon system startup and restart, upon</p>			X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	command from a user with appropriate privilege, and periodically at the frequency defined in the SSP and notifies the System Administrator, shuts the system down, restarts the system or takes appropriate action as defined by the OU when anomalies are discovered. The DOC requires the OUs to employ automated mechanisms to provide notification of failed automated security tests.			
SI-6.2	Automation Support for Distributed Testing The DOC requires the OUs to employ automated mechanisms to support management of distributed security testing.			X
Software and Information Integrity				
SI-7	Software, Firmware, and Information Integrity The DOC requires the OUs to ensure the information system detects and protects against unauthorized changes to software, firmware, and information.		X	X
SI-7.1	Integrity Checks The DOC requires the OUs to reassess the integrity of software, firmware, and information by performing integrity scans of the system at least semi-annually.		X	X
SI-7.3	Centrally-Managed Integrity Tools The DOC requires the OUs to employ centrally managed integrity verification tools.			X

4.19 Program Management (PM)

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
Information Security Resources				
PM-3	Information Security Resources The DOC requires OUs to follow OMB Budget Data Request requirements provided by DOC for reporting IT Security expenditures.	X	X	X
Plan of Action and Milestones Process				
PM-4	Plan of Action and Milestones Process <i>Refer to CITR-018: IT Security Plans of Action and Milestones (POA&M) for control details.</i>	X	X	X
Information System Inventory				
PM-5	Information System Inventory OUs must enter all FISMA-reportable systems into CSAM, review their inventory at least once a fiscal	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	year, and make updates as necessary.			
Information Security Measures of Performance				
PM-6	Information Security Measures of Performance OUs must provide FISMA and CyberCAP metrics per DOC OCS guidance, as well as their own OU-defined performance measures, as appropriate.	X	X	X
Critical Infrastructure Plan				
PM-8	Critical Infrastructure Plan The DOC requires OUs to address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	X	X	X
Risk Management Strategy				
PM-9	Risk Management Strategy The DOC requires OUs to develop and maintain a risk management strategy consistent with CITR-019: <i>Risk Management Framework (RMF)</i> , review it annually, and update it as needed.	X	X	X
Security Authorization Process				
PM-10	Security Authorization Process The DOC requires OUs to designate individuals to fill specific roles and responsibilities within the organizational risk management process. <i>Refer to CITR-019: Risk Management Framework (RMF) for control details.</i>	X	X	X
Insider Threat Program				
PM-12	Insider Threat Program The DOC requires OUs to implement an insider threat program that includes a cross-discipline insider threat incident handling team. DOC OUs follow guidance provided by the Office of Cyber Security and OSY for the fulfillment of this control.	X	X	X
Information Security Workforce				
PM-13	Information Security Workforce <i>Refer to CITR-006: Information Systems Security Training for Significant Roles for control details.</i>	X	X	X
Testing, Training, and Monitoring				
PM-14	Testing, Training, and Monitoring <i>Refer to CITR-006: Information Systems Security Training for Significant Roles, CITR-015: Contingency Plan Testing and Exercise Activities, and CITR-019: Risk Management Framework</i>	X	X	X

Control Number	Control Name/Requirement	Security Baselines		
		Low	Moderate	High
	(RMF) <i>for control details.</i>			
Threat Awareness Program				
PM-16	Threat Awareness Program The DOC requires OUs to implement a threat awareness program that includes a cross-organization information-sharing capability.	X	X	X

Appendix A: Acronyms and Abbreviations

Acronym	Definition
A&A	Assessment and Authorization
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
BPO	Bureau Procurement Official
CAC	Common Access Card
CAM	Commerce Acquisition Manual
CAR	Commerce Acquisition Regulation
CFO	Chief Financial Officer
CIAO	Chief Infrastructure Assurance Officer
CIO	Chief Information Officer
CIPM	Critical Infrastructure Protection Manager
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CITR	Commerce Information Technology Requirement
CITRB	Commerce Information Technology Review Board
CO	Contracting Officer
COOP	Continuity of Operations Planning
COTR	Contracting Officer Technical Representative
CPIC	Capital Planning and Investment Control
CRMO	Compliance & Risk Management Officer
CSAM	Cyber Security Assessment and Management
DAO	Department Administrative Order
DATO	Denial of Authority to Operate
DOC	Department of Commerce
DOO	Department Organization Orders
DoS	Denial of Service
EA	Enterprise Architecture
EIT	Electronic and Information Technology
EO	Executive Order
FACA	Federal Advisory Committee Act
FAR	Federal Acquisition Regulation
FedCIRT	Federation of Computer Incident Response Teams
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom Of Information Act
GAO	Government Accountability Office

Acronym	Definition
HCO	Head of Contracting Office
HSPD	Homeland Security Presidential Directive
ID	Identification
IDS	Intrusion Detection System
IO	Information Officer
ISA	Interconnection System Agreement
ISSO	Information System Security Officer
IT	Information Technology
ITSCC	Information Technology Security Coordinating Committee
ITSO	Information Technology Security Officer
ITSPP	Information Technology Security Program Plan
LO	Line Office
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards & Technology
NIST SP	NIST Special Publication
OAM	Office of Acquisition Management
OCS	Office of Cyber Security
OFM	Office of Financial Management
OGC	Office of General Counsel
OHRM	Office of Human Resource Management
OIG	Office of Inspector General
OLIA	Office of Legislative and Intergovernmental Affairs
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
OPSP	Office of Policy and Strategic Planning
OS	Office of the Secretary
OSY	Office of Security
OU	Operating Unit
P2P	Peer to Peer
PD	Presidential Directive
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PM	Procurement Memorandum
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
RoB	Rules of Behavior

Acronym	Definition
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SAP	Security Accreditation Package
SAR	Security Assessment Report
SCA	Security Controls Assessor
SHRO	Servicing Human Resources Office
SO	System Owner
SP	Special Publication
SSN	Social Security Number
SSP	System Security Plan
U.S.	United States
US-CERT	United States-Computer Emergency Readiness Team
WAC	Web Advisory Council

Appendix B: Glossary

Refer to Appendix B of NIST SP 800-53 Rev. 4 for a full glossary of terms used in that document's security controls.

Term	Definition
Access Control	The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.
Agency	In the context of this document, the term "agency" almost always refers to the Department of Commerce, unless otherwise specified.
Assessment	Usually refers to a <i>Security Assessment</i> (see below), unless otherwise specified.
Assessment and Authorization (A&A)	The process of conducting a security assessment on a system (see <i>Security Assessment</i> below) and determining, based on the results of that assessment, whether the system should be given authorization to operate.
Audit	The independent examination of records and activities to ensure compliance; establish controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Authentication	[FIPS 200] Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Examples of authentication include: showing an ID badge to a security guard; entering a username and password to access a system; and using a PIV badge and PIN to unlock a computer.
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Also called <i>accreditation</i> .
Authorization	The granting of access rights to a user, program, or process. See also <i>Authorization (to operate)</i> and <i>Authorization and Accreditation</i> for authorization specific to information systems.
Availability	The property of a system or service that ensures timely and reliable access to and use of that system or service and the information it contains.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).

Term	Definition
Bureau	See <i>Operating Unit</i> .
Classified Information	Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD). Classified information is not within the scope of this document.
Common Control	[NIST SP 800-37; CNSSI 4009] A security control that is inheritable by one or more organizational information systems. See <i>Security Control Inheritance</i> .
Confidentiality	The property of a system or service that preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Management	The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the development and operational life of the system.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.
Continuity of Operations Planning (COOP)	A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with Emergency Plan, Business Resumption Plan (BRP), and Business Continuity Plan (BCP).
Contractor Operation	An arrangement wherein a third party is contracted by DOC to: <ol style="list-style-type: none"> 1. Provide IT services and systems on behalf of Commerce at contractor facilities; 2. Provide IT services and systems to Commerce via remote access; and 3. Develop or maintain Commerce IT systems or software.
Countermeasures	[CNSSI 4009] Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Denial of Service (DoS)	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. For example, <ul style="list-style-type: none"> • An attacker sends specially crafted packets to a Web server, causing it to crash. • An attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization's network.

Term	Definition
Developer	A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; (iv) and product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.
DOC-Owned/Furnished Resources	DOC-owned/furnished resources are government equipment including computers, other hardware devices, software, and data that are owned by the DOC and are provided to remote users for use in their official duties.
Enterprise	[CNSSI 4009] An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See <i>Organization</i> .
Enterprise Architecture	[44 U.S.C. Sec. 3601] A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
Event	[CNSSI 4009, Adapted] Any observable occurrence in an information system.
External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
Firewall	A firewall is a general term for a network perimeter or border router device (may be hardware, software, or both) designed to prevent unauthorized access to or from one networked environment to another networked environment. A computing environment may consist of one or more firewall devices that each protects specific segments of the internal DOC networked environment. The outermost of these devices would face the public Internet. Firewalls can be configured to examine all messages entering or leaving a DOC network and block those messages that are not explicitly allowed by the firewall configuration rules.

Term	Definition
Firmware	[CNSSI 4009] Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
Hardware	[CNSSI 4009] The physical components of an information system. See <i>Software</i> and <i>Firmware</i> .
Hybrid Security Control	[CNSSI 4009] A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See <i>Common Control</i> and <i>System-Specific Security Control</i> .
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Incident	[FIPS 200] An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information	[CNSSI 4009] Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. [FIPS 199] An instance of an information type.
Information Resources	[44 U.S.C. Sec. 3502] Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.
Information Security Risk	See <i>Risk</i> .

Term	Definition
Information Sensitivity	Information sensitivity reflects the relationship between the characteristics of the information processed (e.g., personnel data subject to protection under the Privacy Act) and the mission need to ensure the confidentiality, integrity, and availability of the information (e.g., legal requirements to protect confidentiality of personal data). Sensitivity may vary from Low, to Moderate, to High (as defined in FIPS 199). During the system risk assessment, the SO must determine the sensitivity, or reaction, of the agency's mission to compromises of confidentiality, integrity, and availability of the information stored and processed by the system. This determination, along with the likelihood of compromise occurring, establishes the level of security adequate to protect the data as required by OMB Circular A-130, Appendix III. The SO must identify the management, technical, and operational controls necessary to provide the required protection, and properly mark media containing sensitive information.
Information System	[44 U.S.C., Sec. 3502] A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
Information System Component	[NIST SP 800-128, Adapted] A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Information System Service	A capability provided by an information system that facilitates information processing, storage, or transmission.
Information System-Related Security Risks	Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See <i>Risk</i> .

Term	Definition
Information Technology (IT)	[40 U.S.C. Sec. 1401 – recodified as 40 U.S.C. Sec. 11101] Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term <i>information technology</i> includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Integrity	The property of a system or service that guards against unauthorized modification or destruction of information (intentional or otherwise). Includes ensuring information non-repudiation and authenticity.
Internal Network	A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
IT Resources	IT resources consist of computer hardware, software, firmware, electronic data, networks, and support for these assets.
IT System	See <i>Information System</i> .
Label	A mean of marking removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.
Line Office	The Line Offices represent the operating branches of NOAA and are responsible for managing the delivery of products and services to meet the needs of the agency’s customers and stakeholders. NOAA’s LOs are accountable for aligning their efforts with respect to particular strategic goals and objectives.
Local Access	Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. Opposite of remote access.

Term	Definition
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Managed Interface	An interface within an information system that provides boundary protection capability using automated mechanisms or devices.
Marking	See <i>Security Marking</i> .
Media	[FIPS 200] Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.
Multifactor Authentication	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See <i>Authenticator</i> .
Network	[CNSSI 4009] Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Term	Definition
Non-Organizational User	A user who is not an organizational user (including public users).
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Operating Unit	As defined by DOO 1-1, the operating units of the Department are organizational entities outside the Office of the Secretary charged with carrying out specified substantive functions (i.e., programs) of the Department.
Organization	[FIPS 200, Adapted] An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).
Organizational User	An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.
Password	A protected/private character string used to authenticate an identity.

Term	Definition
Personally Identifiable Information (PII), Sensitive	<p>Sensitive PII is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Further, in determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a government newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. As well as context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother's maiden name, but each of these elements would not be sensitive independent of one another.</p> <p>For the purpose of determining which PII may be electronically transmitted, the following types of PII are considered sensitive when they are associated with an individual. Secure methods must be employed in transmitting this data when associated with an individual:</p> <ul style="list-style-type: none"> • Place of birth • Date of birth • Mother's maiden name • Biometric information • Medical information, except brief references to absences from work • Personal financial information • Credit card or purchase card account numbers • Passport numbers • Potentially sensitive employment information, e.g., personnel ratings, disciplinary actions, and result of background investigations • Criminal history • Any information that may stigmatize or adversely affect an individual. <p>This list is not exhaustive, and other data may be sensitive depending on specific circumstances.</p> <p>Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed.</p>

Term	Definition
Personally Identifiable Information (PII), Non-Sensitive	<p>The following additional types of PII may be transmitted electronically without protection because they are not considered sufficiently sensitive to require protection.</p> <ul style="list-style-type: none"> • Work, home and cell phone numbers • Work and home addresses • Work and personal e-mail addresses • Resumes that do not include an SSN or where the SSN is redacted • General background information about individuals found in resumes and biographies • Position descriptions and performance plans without ratings <p>The determination that certain PII is non-sensitive does not mean that it is publicly releasable.. The determination to publicly release any information can only be made by the official authorized to make such determinations. The electronic transmission of non-sensitive PII is equivalent to transmitting the same information by the U.S. mail, a private delivery service, courier, facsimile, or voice. Although each of these methods has vulnerabilities, the transmitted information can only be compromised as a result of theft, fraud, or other illegal activity.</p>
Physical Access Control Mechanism	An automated or manual system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
Plan of Action and Milestones (POA&M)	[OMB Memorandum 02-01] A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact	[FIPS 199] The loss of confidentiality, integrity, or availability could be expected to have: (i) a <i>limited</i> adverse effect (FIPS Publication 199 low); (ii) a <i>serious</i> adverse effect (FIPS Publication 199 moderate); or (iii) a <i>severe</i> or <i>catastrophic</i> adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.

Term	Definition
Privacy Impact Assessment (PIA)	[OMB Memorandum 03-22] An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Account	An information system account with authorizations of a privileged user.
Program Office	An organizational unit within an OU that exists to fulfill a unique function/mission (e.g. Acquisitions).
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). Remote access uses telecommunications to enable authorized access to non-public DOC computing services that would otherwise be inaccessible from work locations outside a DOC LAN or DOC-controlled WAN computing environment. This includes access to non-public DOC IT systems and data that are exposed to the public Internet (e.g., web access to electronic mail by the home user or business traveler) as well as modem dial-up and/or Virtual Private Network (VPN) access to internal DOC IT servers and desktop workstations.
Residual Risk	The remaining risk not eliminated by implementation of security controls or countermeasures.
Risk	<p>[FIPS 200, adapted] A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.</p> <p>Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.</p>

Term	Definition
Risk Assessment	<p>The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.</p> <p>Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.</p>
Risk Management	[CNSSI 4009, adapted] The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Mitigation	[CNSSI 4009] Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
Security	[CNSSI 4009] A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Security Assessment	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security Assessment Report (SAR)	DOC-mandated documentation of findings in a risk assessment.
Security Authorization	See <i>Authorization</i> .
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See <i>Security Category</i> .

Term	Definition
Security Category	[FIPS 199, Adapted; CNSSI 4009] The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.
Security Control	[FIPS 199, Adapted] A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Control Assessor (SCA)	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline	[FIPS 200, Adapted] The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.
Security Control Enhancement	Augmentation of a security control to: (i) build in additional, but related, functionality to the control; (ii) increase the strength of the control; or (iii) add assurance to the control.
Security Control Inheritance	[CNSSI 4009] A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See <i>Common Control</i> .
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis	[CNSSI 4009] The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Incident	See <i>Incident</i> .

Term	Definition
Security Marking	The means used to associate a set of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies.
Security Objective	[FIPS 199] Confidentiality, integrity, or availability.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Requirement ²	[FIPS 200, Adapted] A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.
Security Service	[CNSSI 4009] A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.
Sensitive Information	Any information of which the loss, misuse, modification, or unauthorized access could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an EO or an act of Congress to be kept classified in the interest of national defense or foreign policy.
Software	[CNSSI 4009] Computer programs and associated data that may be dynamically written or modified during execution.
Supplemental Guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
Supplementation	The process of adding security controls or control enhancements to a security control baseline as part of the tailoring process (during security control selection) in order to adequately meet the organization's risk management needs.
Supply Chain	[ISO 28001, Adapted] Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

² Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.

Term	Definition
System	See <i>Information System</i> .
System of Records Notice (SORN)	An official public notice of an organization's system(s) of records, as required by the Privacy Act of 1974 that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.
System Owner (SO)	Mid-level manager responsible for day-to-day system operations and responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
System Security Plan (SSP)	[NIST SP 800-18] Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to a security control baseline. See <i>Tailoring</i> .
Tailoring	The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. They consist of: identification and authentication; access control; audit and accountability; and system and communications protection.
Threat	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or DoS.

Term	Definition
Trustworthiness (Information System)	<p>The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.</p>
Unauthorized Access	<p>A person gains logical or physical access without permission to a network, system, application, data, or other resource. For example,</p> <ul style="list-style-type: none"> • An attacker runs an exploit tool to gain access to a server's password file. • A perpetrator obtains unauthorized administrator-level access to a system and then threatens the victim that the details of the break-in will be released to the press if the organization does not pay a designated sum of money.
User	<p>Person or process accessing an information system either by direct connections (e.g., via terminals), or indirect connections (e.g., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).</p>
Vulnerability	<p>[CNSSI 4009] Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.</p>



Department of Commerce

Commerce Information Technology Requirement

CITR-016
January 25, 2012

Vulnerability Scanning and Patch Management

1. PURPOSE

This policy modifies DOC Information Technology Security Program Policy (ITSP) requirements for vulnerability scanning and patch management.

2. BACKGROUND

Vulnerability scanning provides a key mechanism to identify security weaknesses and correct these weaknesses by system upgrades or patches, before they can be exploited. Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with, or deviations from, an Operating Unit's (OU) security policy. Patch management provides a means of both remediating and preventing security vulnerabilities. In 2011, the Office of Management and Budget (OMB) issued Memorandum 11-33, "*FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*" providing new Federal Information Security Management Act (FISMA) reporting metrics, including requirements for agencies to report: 1) the number of network connected Information Technology (IT) assets; and 2) the number of IT assets where an automated capability provides visibility at the agency level into detailed vulnerability information. OUs are advised to consider CITR-017 regarding Security Configuration Checklist Program requirements when planning for the implementation of this policy.

3. SCOPE

These minimum requirements apply to all information systems owned by or operated on behalf of DOC where the Department has the legal and/or contractual authority to dictate requirements.

4. AUTHORITY

The DOC Chief Information Officer (CIO) has the authority to develop, implement, and manage IT security processes and procedures to protect the availability, confidentiality, and integrity of the Department's IT resources. The DOC Chief Information Security Officer (CISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and FISMA; with regulatory requirements and external guidance, including OMB policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirements.

5. CANCELLATION/AUGMENTATION OF EXISTING POLICY

This policy replaces ITSPP Section 4.14.4 (Vulnerability Scanning) and provides additional requirements for patch management. It also replaces CITR-003 Continuous Monitoring Plan, dated 12/19/08, Section 6.F.

6. REQUIREMENTS

- A. OUs must establish dedicated resources for vulnerability scanning and patch management.
- B. OUs must perform vulnerability scans of network-addressable IT assets at least quarterly.
- C. At a minimum, scanning must identify active IP addresses, MAC addresses (or other hardware identifier), operating systems, general purpose applications, open ports, services, vulnerabilities, and missing patches.
- D. Tools used to perform scanning must be Security Content Automation Protocol (SCAP) compliant when available.
- E. OUs must perform credentialed vulnerability scanning. The OU must ensure that administrative accounts with sufficient privileges are enabled to allow the scanning device to inspect all security related elements of each network addressable device within a system boundary.
- F. OUs shall implement processes incorporating the following parameters to ensure the timely remediation of vulnerabilities:
 - 1. Vulnerabilities shall be remediated within 30 days of discovery for FIPS 199 high impact systems, 60 days for moderate impact systems, and 90 days for low impact systems.
 - 2. The National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) shall be used to provide a score for vulnerabilities as a 'low', 'medium', 'high', or 'critical' severity level.
 - 3. Timeframes for remediation may be modified as appropriate based on the impact level of the system, vulnerability, compensating controls, and likelihood of exploit.
 - 4. Vulnerability remediation actions must be documented in Plans of Action and Milestones (POA&M).
- G. OUs shall consider invoking penalties for non-remediation of vulnerabilities.
- H. Authorizing Officials (AO) or their designees shall manage, accept, and document risks introduced when remediation of vulnerabilities identified cannot be performed as anticipated.

- I. Per the DOC ITSP, OUs are required to comply with CITRs within 90 days, or as stipulated in the CTR. Compliance with CTR requirements beyond the specified timeframe shall be managed through the use of POA&Ms.

7. REFERENCES

M-11-33 and FISIM 11-02: Memorandum for Heads of Executive Departments and Agencies FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management: <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf>.

NVD Common Vulnerability Scoring System Support v2: <http://nvd.nist.gov/cvss.cfm>.

Simon Szykman

Chief Information Officer





Herbert Clark Hoover Building OCIO Change Control Board Charter

**Version 3
February 5, 2015**

Document Details

Business Owner	Audience	Creation Date
Jun Kim	Herbert Clark Hoover Building	20130326

Revision History

Date	Version	Description	Author
20130617	1.0	HCHB Change Control Board Charter	J. Kim
20130717	1.01	Copy edits and formatting changes. Also added Table of Contents, Glossary and Appendix A.	A. Jones
20130718	1.02	Revised Emergency change definition and review process.	J. Kim
20130806	1.03	Inserted approval line for the CTO/DCIO	J. Kim
20140109	2.0	Revised voting members and decision making process, added Appendix for charter acceptance	J. Kim
20140110	2.0	Minor edits and formatting	A. Jones
20141212	3.0	Process Update to include change closure, monthly maintenance window, and emergency reporting process. Escalated authority level from CTO to CIO.	J. Kim
20141222	3.1	Corrected section numbering and TOC	J. Kim
20141224	3.2	Minor formatting and edits to acronyms	J. Kim
20150105	3.3	Minor edits and formatting	A. Jones
20150205	3.4	Process owner designation change	J. Kim

Document Approvals

Name	Title	Role
Steve Cooper	Chief Information Officer, U.S. Department of Commerce	Executive Sponsor
Jun Kim	Chief, Security Operations Center	Change Management Process Owner/Change Manager

Steve Cooper
Chief Information Officer, DOC

Date

Jun Kim
Chief, Security Operations Center

Date

Contents

1. Purpose.....	5
2. Scope	5
3. Objective.....	6
4. Mission and Guidance.....	6
5. Roles and Responsibilities	6
6. Change Types and Submission Process.....	8
7. Change Review Process	9
7.1 Emergency Changes.....	9
7.2 Change Closure Process.....	9
8. Monthly Maintenance Window	10
9. Scheduled Meetings	10
10. Charter Amendments	11
11. Glossary	12
11.1 Terms.....	12
11.2 Acronyms.....	14
Appendix A – CCB Members.....	15
Appendix B – Bureau and Operating Unit Charter Acceptance	16

1. Purpose

The purpose of the Herbert Clark Hoover Building (HCHB) Change Control Board (CCB) for the U.S. Department of Commerce (DOC) is to establish and maintain the governing body to ensure that configuration changes – including changes to hardware, software and services – do not impair the ability of the DOC Office of the Chief Information Officer (OCIO) to deliver quality IT services to HCHB stakeholders. The CCB is responsible for ensuring changes to systems granted under this authority are correct, consistent, complete, and meet Federal and DOC requirements for IT systems to include voice and data networks.

2. Scope

The CCB currently has authority and governance over changes to production-level infrastructure and enterprise applications and components defined under the following OCIO-managed General Support Systems (GSS):

1. Herbert C. Hoover Building Network (HCHBNet) OS-003
2. Office of IT Services General Support System (OITS GSS) OS-063

Changes made to systems interconnected with HCHBNet not specified above are generally not covered under the scope for this CCB. However, changes to systems that will affect the HCHB shared infrastructure should be submitted for review and will be processed as in-scope. Examples of changes that fall under this criteria include adoption of new technologies requiring a significant increase in bandwidth consumption and opening of non-standard communication ports that may present an increased risk in security posture level for the HCHB infrastructure.

Additionally, requests for changes to staging or development area networks that are considered to be in non-production status attached to the HCHB network infrastructure are not in-scope for this CCB.

The scope of changes reviewed under this board is subject to change as the process matures and as additional systems are added under this authority. Any change outside the scope will be referred to the applicable system owner or to the Director of Office of IT Services (OITS) and DOC CIO as appropriate. Any further questions may be directed to the change management process owner.

3. Objective

The HCHB CCB will meet the objective of establishing a change control process responsible for evaluating change proposals for the systems identified and managed by OCIO. This change evaluation process will help ensure that modifications to these systems are properly addressed, tested, and approved prior to implementation. Additionally, the CCB will provide stakeholders a forum to provide input on changes and to be informed of upcoming maintenance resulting from approved changes that may have an impact to services provided by the OCIO.

4. Mission and Guidance

The CCB is formed to provide an effective and efficient governing body for evaluating system configuration changes and identifying, prioritizing, and managing risks that may be associated with those changes. (Sections 5 and 6 below define the different type of change requests and explain in detail how the CCB handles each.)

5. Roles and Responsibilities

CCB Role	Organizational Title	Voting Member (Y/N)
Chairperson	Change Manager	Y
Advisor	Functional Area Chief	Y
Member	Bureau/OU Representatives	N
Risk Assessment Team	OITS Security, NOC, SOC, ITSD Representatives	N
Documentation Representative	Technical Writer	N

The initial HCHB CCB roles are listed in the table above. While designated individuals may change, these essential roles will continue for the entire life cycle of the CCB. See [Appendix A](#) for the list of personnel assigned to these roles.

Chairperson (backup/alternate)

- Appointed by the OITS Director;
- Maintains and approves members of the CCB;
- Facilitates CCB meetings and agendas as required;
- Ensures the CCB process is followed and aligns with the charter;
- Approves meeting minutes and ensures action items are tracked to completion;
- Approves and rejects change requests based on information and recommendations provided.

Advisor

- Elected by the chairperson;
- Participates in CCB meetings regularly;
- Represents management of functional area involved in the CCB process;
- Reviews and advises the chair on the proposed changes;
- May serve as voting member in the decision process.

Member

- Invited by the chairperson;
- Provides representation of respective bureau;
- Participates in CCB meetings regularly;
- Informs the CCB of upcoming scheduled maintenance or blackout dates to minimize conflict with changes proposed and scheduled by the CCB.

Risk Assessment Team

- Members are appointed by OITS IT Security;
- Performs preliminary risk assessments of all change requests submitted to the board;

- Reviews the details of change requests and provides results from the risk analysis to the CCB;
- Engages appropriate staff from other functional areas and bureaus as required to make an informed recommendation.

Documentation Representative

- The Documentation Representative is responsible for recording and distributing CCB meeting minutes;
- Provides and collects CCB meeting sign-in sheet;
- Develops forms, templates etc. as required for CCB process and procedures.

6. Change Types and Submission Process

The HCHB CCB defines change requests into four different types:

1. **Normal** – Changes that may have a significant impact or risk at the organization level or higher affecting more than one user.
2. **Emergency** – Changes that are required to restore services in order to maintain a Service Level Agreement (SLA) with a customer. See Section 6.1 below for details.
3. **Scheduled** – Non-Emergency changes that impact the availability of services and require broadcast notification of the scheduled maintenance window.
4. **Pre-Approved** – Changes that have been established as regularly performed operational maintenance task items and have little to no impact to the user community.

All changes shall be documented and tracked using the OCIO IT Service Desk (ITSD) ticketing system. Bureaus will continue to follow the standard submission process for submitting a service request. The ITSD may be contacted by email at ITSD@doc.gov or by phone at (202) 482-5010 for additional assistance. The receiving OCIO technical function responsible for performing the configuration change will evaluate and determine the requirements for a formal change request submission and process accordingly.

7. Change Review Process

Changes with the exception of Pre-Approved changes will be subject to formal review by the CCB. Changes categorized as Pre-Approved do not require formal approval by the board. However, these types of changes will be audited by the chairperson and risk assessment team on a monthly basis to ensure consistency and accuracy in classification.

Normal, Emergency, and Scheduled changes will require a risk assessment and CCB review. The individual submitting the change is responsible for presenting and ensuring the parties involved are at the CCB review session.

Each CCB review session will have a quorum of two-thirds of the voting members in attendance; however, the chairperson will have the authority to continue if the quorum is not met. During the review session, the risk assessment team will present their risk analysis and each CCB member and advisor will have an opportunity to provide input. Voting will take place for each change request after it has been reviewed and presented to the board – simple majority is the deciding factor. However, the chairperson does have the authority to override and/or escalate any decision to senior level management. The chairperson will announce the final decision after the vote for each change.

The decision for each change will be tracked in the OCIO ITSD ticketing system and documented in the CCB meeting minutes.

7.1 Emergency Changes

For Emergency changes, the technical group making the change should obtain approval from the System Owner or, alternatively, follow a defined escalation and authorization process prior to implementation. (In the latter case, it is the responsibility of the escalation point-of-contact to assess the implications of the anticipated change.) Nevertheless, Emergency changes are not exempt from the CCB review process. An Emergency change request must be submitted at the time the work-around is implemented, or immediately thereafter the following business day. All Emergency change requests will be summarized and discussed at the next regularly scheduled CCB meeting.

7.2 Change Closure Process

Changes that have been implemented should be updated accordingly in the ITSD ticketing system. Completed test results and lessons learned are to be entered in the change request journal entries and attachment sections. Functional teams

responsible for implementing the change should designate a representative to attend the following CCB meeting to provide a status on the change. Once all action items for the change request have been confirmed, the board will approve the closure of the change and mark the request as completed.

8. Monthly Maintenance Window

To establish change culture in the HCHB computing environment, the CCB has designated the third weekend of each month as a regularly occurring OCIO monthly maintenance weekend with the exception to the month of September due to year end fiscal year financial processing. The maintenance window is established as the third Friday of each month beginning at 9PM EST to the following Sunday at 2AM EST. All changes impacting the HCHB production infrastructure and services will be scheduled during this time including any routine maintenance or testing (e.g. system failover/redundancy testing). Other service impacting changes may continue to occur outside of this maintenance window, however these changes will be declared by the change manager as emergency or critical level changes due to priority and direction from higher executive level authorities.

9. Scheduled Meetings

The CCB will meet weekly unless otherwise noted. The Chairperson or designated backup/alternate will schedule and facilitate the CCB meetings. The Chairperson reserves the right to call an emergency CCB meeting when needed to address any emergency changes needed. If the Chairperson is unable to attend a meeting, the backup or alternate Chairperson is to serve as Chairperson. Any member who cannot attend a regularly scheduled meeting must contact their alternate to attend and ensure the alternate is empowered to address issues before the Board. Voting members and advisors are expected to review the materials before the meeting to facilitate an informed decision making process. The weekly CCB schedule for action items is shown in the table below.

CCB ACTION ITEM	ASSIGNED	WEEKLY DUE DATE
Change Request Submission	Requestor	Thursday, 12PM
Risk Assessment and Review	OCIO Risk Assessment Team	Monday, COB
CCB Meeting	CCB Members and Participants	Tuesday, 2PM - 3PM

*Note: In the event of a federal holiday or closure of the federal government, the schedule above may be shifted to the next business day to allow additional time for review.

10. Charter Amendments

Amendments to this Charter may be made by proposing the change at any regular business meeting. The proposal will be reviewed by the CCB chairperson and advisors and submitted to executive management for final approval.

11. Glossary

11.1 Terms

Bureau Representative: The designated individual with granted authority to represent and make decisions on behalf of his/her respective bureau or operating unit. The individual serves as a middle-man between the customer and the change control board.

Change Control Board: A group of people that assesses, prioritizes, authorizes and schedules changes to the organization's IT infrastructure. The OCIO's Change Control Board meets weekly to consider change requests to the Department of Commerce's IT infrastructure on the HCHB campus. The CCB takes into consideration the potential impact of changes on other services, on shared resources and on the overall change schedule.

Change Request: A formal proposal for a change to be made to an organization's IT infrastructure. It includes details of the proposed change.

Configuration Management: This is the monitoring, documenting and control of how the hardware and software of an organization's IT infrastructure are configured. In other words, it is the management of how an organization's IT assets are setup and operate with one another to provide the services required by IT customers.

Federal Information Systems Management Act: This Act requires each U.S. federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. It includes a number of security standards with which U.S. federal agencies must comply.

HCHB Network: This network serves as the backbone network infrastructure for the local area network (LAN), the Voice over Internet Protocol (VoIP) telephone system, the Emergency Broadcast System (EBS) and the Public Address system for the U.S. Department of Commerce offices in the Herbert C. Hoover Building. The HCHB Network or HCHBNet is maintained by the Office of IT Services, which is part of the Office of the Chief Information Officer.

Herbert C. Hoover Building: This is the building that houses the headquarters for the U.S. Department of Commerce and is located at 1401 Constitution Avenue, N.W., Washington, D.C.

Information Technology Infrastructure Library: This is an internationally recognized framework of IT best practices based on the central principle that information technology should be managed and delivered as a service. It is the framework that has been adopted by the OITS in order to improve the quality and speed of IT services to internal and external customers on the HCHB campus. Reference: <http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx>. (NOTE: This definition is included in this glossary, as ITIL principles play a key role in the deliberations of the Change Control Board.)

IT Service Desk: Often referred to as the "Help Desk," the IT Service Desk is the primary contact between IT customers and the Office of IT Services. It is located in HCHB Room 6071. It can be reached by email at itsd@doc.gov and by phone at 202-582-5010.

Network Operations Center: The organization and the physical workspace for DOC staff and/or contractors who provide network installation, maintenance and support.

Service Desk: This is the Office of the Secretary Information Technology Service Desk (OS IT Service Desk). It is also known as the "the Help Desk," which is actually a misnomer. The Service Desk responds to requests for technical assistance such as new user account setups and hardware and software installations. The Desk also handles hardware and software issues for end users.

Security Operations Center: This organization monitors and protects the data networks on the HCHB campus against internal and external Information security threats while providing a safe computing environment that enables each operating unit to pursue its business objectives within the framework of FISMA.

11.2 Acronyms

CCB: Change Control Board

CR: Change Request

DOC: Department of Commerce

HCHB: Herbert C. Hoover Building

HCHBNet: HCHB Network

ITCSC: Information Technology Customer Service Center

ITSD: IT Service Desk

NOC: Network Operations Center

OCIO: Office of the Chief Information Officer

OFM: Office of Financial Management

OITS: Office of IT Services (formerly ONTO – Office of Networking and Telecommunications Operations)

OS: Office of the Secretary of the U.S. Department of Commerce

SOC: Security Operations Center

Appendix A – CCB Members

The following table lists the members of the Change Control Board as of January 2015.

CCB Role	Organizational Title	Bureau/OU	Current Member
Chairperson	Change Manager/Chief Security Operations Center	OS/OITS	Jun Kim
Backup Chair	Chief, Enterprise Systems Engineering	OS/OITS	Wes Ky
Advisor	OS IT Security Officer	OS/OITS	Amy Hintz
Advisor	Chief, Customer Services/Service Desk	OS/OITS	Erin Cavanaugh
Advisor	Chief, Enterprise Applications	OS/OITS	Dennis Sutch
Advisor	Chief, Enterprise Architecture	OS/OITPP	Tom Pennington
Advisor	Manager, Voice Operations	OS/OITS	Demetria Blyther
Member	OU/Bureau Representative	HCHB OUs	Appointed Bureau/OU representative
Risk Assessment Team	OCIO OITS Security	OS/OITS	Rick Anderson (Lead), Jerome Madden (Alternate)
Documentation Representative	Technical Writer, OITS	OS/OITS	Alexander Jones

[Go to Section 5: Roles and Responsibilities](#)

Appendix B – Bureau and Operating Unit Charter Acceptance**X**

Eddie Donnell
BIS Executive Sponsor

X

Daniel Drew
NTIA Executive Sponsor

X

Joe Paiva
ITA Executive Sponsor

X

Abdil Salah
OIG Executive Sponsor

X

Zachary Goldstein
NOAA Executive Sponsor

X

Mark Johnson
EDA Executive Sponsor

X

James Gwinn
NTIA FirstNet

X

Steve Cooper
OS, EDA, ESA, MBDA Executive Sponsor

Server Operating System	Count	TOTAL	Total Active
Microsoft Windows Server 2008	5	14	8
Microsoft Windows Server 2012	0		
Microsoft Windows Server 2003	6		
Linux/Unix	3		

Location	Operating System Name	Device Name	Server Type (Virtual/Physical)	Application/Purpose	Active/Storage/ Retired
Room A001	Microsoft Windows Server 2008	HCHBCMMENT	P	Men&Mice Server	Active
HCHB Data Center	Microsoft Windows Server 2008	HCHBNOCTEST	P	NOC Test Server	Active
HCHB Data Center	Microsoft Windows Server 2008	HCHBNOCDC3	P	HCHBNOC Domain Controller	Active
HCHB Data Center	Microsoft Windows Server 2008	Tape Robot	P	Storage	Retired
HCHB Data Center	Linux	HCHBLA1	P	Firewall Log Server	Retired
HCHB Data Center	Linux	NEWDNS1	P	DNS Server	Active
HCHB Data Center	Linux	HCHBNOC1	P	HCHBNOC Domain Controller	Retired
HCHB Data Center	Microsoft Windows Server 2003	HCHBIPS1	P	DHCP Server	Retired
HCHB Data Center	Microsoft Windows Server 2008	HCHBBKP1	P	Storage	Retired
Room A001	Microsoft Windows Server 2003	HCHBIPS2	P	DHCP Server	Retired
Room A001	Microsoft Windows Server 2003	HCHBSYSLOG1	P	Kiwi Server	Retired
Room A001	Microsoft Windows Server 2003	HCHBNOC3	P	HCHBNOC Domain Controller	Retired
Room A001	Microsoft Windows Server 2003	HCHBEXAGRID2	P	Storage	Retired
Room A001	Microsoft Windows Server 2003	HCHBEXAGRID1	P	Storage	Retired

Name	Description
SolarWinds IP Address Manager IPX (unlimited IPs)	IP address management and administration
Redhat Maintenance (SOC)	Linux Support Subscription
vRealize	Virtual environment operations and automation
Informcast (Singlewire - Berbee)	A full-featured emergency notification solution that enables people to reach an unlimited number of Cisco IP phones, speakers, cell phones, and other devices with text and live, ad-hoc, pre-recorded, or text-to-speech audio
Men & Mice	DNS, DHCP, & IP Address Management solutions for Microsoft Active Directory and UNIX based IP networks.
Infortel	Software that enables call monitoring, recording, process automation, business metrics; search, retrieval, playback, and export of calls.
CommVault Simpana 10	Performs back-ups for DOC Private Cloud
Air Magnet	Software that is used for wireless surveys, measurement of wireless network performance metrics, and troubleshooting of wireless networks
Solarwinds Toolkit	Network Management Tool for the Hnet Management Block
SolarWinds Monitoring tool	System Monitoring
Solar Winds Net Flow Traffic Analyzer	Network Utilization, Reporting, Packet Inspection, and Application Inspection
VOIP and Network Quality Manager IP SLA	Jitter, packet loss, latency
APC StruxtureWare	APC Monitoring Tool
McAfee MFE, AntiVirus, VirusScan, Internet Security	
Data Mountain DNS	Private Cloud DNSSEC Self Signing Service of Secondary Zone Hosting for 28 DoC Domains, with FISMA compliant Monitoring & Reporting
VM Ware Vsphere (64 licenses)	Virtual environment computing virtualization platform
VMWARE VCENTER SVR 5	
VM Ware Vsphere (16 licenses)	Centralized platform for managing VMware vSphere environments
SolarWinds Network Configuration Manager DL3000	Configuration management
SolarWinds User Device Tracker UTX (unlimited ports per server)	Endpoint device search, vendor identification, rogue device detection, performance and capacity reporting
RSA Authentification Manager	The central two-factor authentication software that provides capabilities to manage security tokens, users, multiple applications, agents, and resources across physical sites.
Entrust SSL Certificate	Certificate for ASA Firewalls
Cisco Jabber	Access presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing.

[illegible]

HCHB Data Center	Name of Device	POWER CONNECT M6348	Serial Number	Active/Storage/ Retired
HCHB Data Center	Websense URL Network Agent 784	Dell PowerEdge R710 - Windows 2008 R2		Active
A001	Websense V10000 Secondary 784	Websense Appliance		Active
HCHB Data Center	Websense V10000 Primary 784	Websense Appliance		Active
A001	Websense Inside Agent 784	Dell PowerEdge R710		Active
HCHB Data Center	Websense Inside Agent 784	Dell PowerEdge R710		Active
HCHB Data Center	Websense URL Network Agent	Dell PowerEdge 1950 - 2.5 GHz Xeon, 8 GB RAM, 136 GB HD		Active
A001	Websense URL Network Agent	Dell		Active
HCHB Data Center	Websense V10000 Appliance	Websense Appliance		Active
A001	Websense V10000 Appliance	Websense Appliance		Active
HCHB Data Center	Websense V5000 Appliance	Websense Appliance		Active
A001	Websense V5000 Appliance	Websense Appliance		Active
HCHB Data Center	Websense DLP Protector (Open Office Printer)	Dell PowerEdge 1950 - Windows 2008 R2 ENT 2.2 GHz Xeon, 4 GB RAM, 136 GB HD		Active
HCHB Data Center	Websense DLP Protector (Inside)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
HCHB Data Center	Websense DLP Protector (Remote)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
HCHB Data Center	Websense DLP Protector (G2G)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
HCHB Data Center	Websense DLP Protector (PDMZ)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
A001	Websense DLP Protector (G2G)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
A001	Websense DLP Protector (Inside)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
A001	Websense DLP Protector (PDMZ)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
A001	Websense DLP Protector (Remote)	Dell PowerEdge 1950 - 2.2 GHz Xeon, 4 GB RAM, 136 GH HD		Active
HCHB Data Center	Tenable Scanner Appliance	Proprietary		Active
HCHB Data Center	Physical Passive Vulnerability System	Dell PE R710		Active
	Tenable Passive Scanner (Virtual)	Virtual		Active
HCHB Data Center	Primary Intrushield Sensor	McAfee Intrushield I-4010		Active
A001	Secondary Intrushield Sensor	McAfee Intrushield I-4010		Active
HCHB Data Center	McAfee ETM-6000G	Threat Manager		Active
HCHB Data Center	McAfee ELM-6000G	Log Manager		Active
HCHB Data Center	McAfee ACE-2600	Advanced Correlation Engine		Active
HCHB Data Center	McAfee ERC-2600	Receiver		Active
HCHB Data Center	McAfee ERC-2600	Receiver		Active
HCHB Data Center	Secondary NSM	Dell PowerEdge R430		Active

[illegible]

KEY PERSONNEL QUALIFICATIONS MATRIX

Proposed Personnel Name:

Proposed Personnel Employer:

Proposed Position:

Proposed Labor Category:

Clearance Level: (i.e. Not a requirement for this position, Secret, ect.)

Requirements	Place of work & client if appropriate	Dates for cited experience	Years of experience for each cited position held	Official title for each cited position held	Description of qualifications for <u>each</u> cited position held

Note: Multiple pages for qualifications are acceptable.

REQUEST TO INITIATE PURCHASE (RIP) FOR EQUIPMENT, MATERIALS, OTHER DIRECT COSTS (ODCs), AND/OR SERVICES

If the prime contractor has an approved purchasing system, the contractor shall prepare and submit a RIP to be reviewed and signed by the GSA COR.

Contractor:	RIP Number:	
Client:	Date:	
	Project Name:	
	Project/Interagency Agreement (IA) Number:	
	Associated Line of Accounting:	
	Task Order Number:	

TO:	(Insert First and Last Name) , GSA Contracting Officer's Representative (COR)	CLIN X00X VALUE:	\$	-	Last Invoice submitted:
FROM:	(Insert First and Last Name of requestor)	CUMULATIVE AMOUNT BILLED:	\$	-	
THROUGH:	(Insert client organization and First and Last Name) , Technical Point of Contact GTR	CURRENT CLIN X00X BALANCE:	\$	-	
		RIP ESTIMATE:	\$	-	
SUBJECT:	Request to Initiate Purchase # (insert number)	NEW CLIN X00X BALANCE:	\$	-	
DATE:	(Insert Month Date, Year)				

PURPOSE/JUSTIFICATION OF REQUEST:

ESTIMATED PURCHASE COST:

Item: (insert item(s))	
Item Cost	\$ -
Indirect costs authorized by the Task Order (insert as appropriate)	\$ -
Total Not to Exceed (NTE) cost	\$ -

All equipment, materials, and ODCs shall be purchased in accordance with client requirements. All equipment, materials, and ODCs shall become the property of the Government and shall be regarded as Government Furnished Property (GFP), and unless previously approved by the Contracting Officer, shall be used only in performance of this Task Order. All materials shall be purchased in accordance with applicable Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) clauses (choose as appropriate) and approved purchasing procedures. All equipment, materials, and ODCs shall be purchased in accordance with Task Order requirements and shall not exceed the funded amount on this Task Order. The contractor shall ensure that the prices quoted are fair and reasonable at the time of submission and are in the best interest of the Government.

Please contact me at (area code) 000-0000 (insert requestor's phone number) if you have any concerns or questions.

GSA COR Approval:	
Signature	Date

CONSENT TO PURCHASE PARTS/TOOLS/ODCs AND/OR SERVICES (CTP)

Industry Partner:	TOOL#:	
Client:	Date:	
	Project Name:	
	Project/IA#:	
	Contract/Task Order:	

If the prime contractor does not have an approved purchasing system, the contractor will prepare and submit a Consent to Purchase (CTP), to be reviewed by the COR and signed by the CO.

TO:	GSA Contracting Officer Representative	CLIN # VALUE:	\$0.00
		CUM AMT BILLED:	\$0.00
		BALANCE:	\$0.00
FROM:	Requestor	CTP ESTIMATE:	\$0.00
THROUGH:	Client POC	BALANCE:	\$0.00
SUBJECT:	Consent to purchase #		

Client Point of Contact:

PURPOSE/JUSTIFICATION OF REQUEST:

The purpose of this request is to

Description of supplies or sevicees (FAR 52.244-2(e)(1)(i)):

Type of subcontract (FAR 52.244-2(e)(1)(ii)):

Propose subcontractor (FAR 52.244-2(e)(1)(iii)):

Below is the estimated cost of purchase (FAR 52.244-2(e)(1)(iv)):

ITEM	
Tool (CLIN #):	
Cost to Government: @#	\$ -
Fee	\$ -
General & Administrative (G&A) Cost	\$ -
Total Cost NTE:	\$ -

All material purchases shall be made in accordance with customer requirements. All materials shall become the property of the Government and shall be regarded as Government Furnished Property (GFP), and unless previously approved by the Contracting Officer, shall be used only in performance of this Task Order. All materials will be purchased in accordance with regulations contained in FAR 52.244-2 approved purchasing procedures. All Tools and ODCs shall be procured in accordance with contract requirements and shall not exceed the funded amount on this contract.

It is the responsibility of the Industry Partner to ensure that the prices quoted are fair and reasonable at the time of submission and are in the best interest of the client. The Industry Partner is to furnish price quotes for hardware and software purchases.

- The following documents are attached (as necessary):
- 1) Subcontractor's certified cost or pricing data as required in FAR 52.244-2(e)(1)(v)
 - 2) Subcontractor's Disclosure Statement or Certification relating to Cost Accounting Standards as required in FAR 52.244-2(e)(1)(vi)
 - 3) Negotiation memo as required in FAR 52.244-2(e)(1)(vii)

Please contact me at (000) 000-0000 if you have any concerns or questions.

GSA CO Approval:

Signature

Date

Corporate Non-Disclosure Agreement

AN AGREEMENT BETWEEN [INSERT NAME OF CONTRACTOR]
AND THE UNITED STATES

1. Intending to be legally bound, [INSERT NAME OF CONTRACTOR] hereby accepts the obligations contained in this agreement in consideration of [INSERT NAME OF CONTRACTOR] being granted access to sensitive data. As used in this Agreement, sensitive data is marked or unmarked "sensitive but unclassified information" (SBU), including oral communications, that meets the standards set by Office of Management and Budget (OMB) Circular A-130 Appendix 3 and DOC. I understand any data or systems of records protected from unauthorized disclosure by the provisions of Title 5, United States Code Sections 552 (often referred to as ("The Freedom of Information Act") and 552a ("The Privacy Act") is/are sensitive data. In addition, other categories of information, including but not limited to medical, personnel, financial, investigatory, visa, law enforcement or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon individual privacy, federal programs, or foreign relations is sensitive data. The term includes data whose improper use or disclosure could adversely affect the ability of the Agency to accomplish its mission, as well as proprietary data and information received through privileged sources. Data of this type which requires protection and limited dissemination must be designated by any official having signing authority for the material. I understand and accept that by [INSERT NAME OF CONTRACTOR] being granted access to sensitive data, special confidence and trust has been placed in me by the United States Government.
2. [INSERT NAME OF CONTRACTOR] acknowledge that it has been given access to DOC's sensitive data to facilitate the performance of duties assigned to it for compensation. [INSET NAME OF CONTRACTOR] understands its responsibility to safeguard sensitive data disclosed to it, and to refrain from disclosure sensitive data to persons not requiring access for performance of official duties. Before disclosing sensitive data, [INSERT NAME OF CONTRACTOR] must determine the recipient's "need to know" or "need to access" sensitive data.
3. [INSERT NAME OF CONTRACTOR] has been advised that any breach of this Agreement may result in the termination of [INSERT NAME OF CONTRACTOR] access to sensitive data, which, if such termination effectively negates [INSERT NAME OF CONTRACTOR] ability to perform assigned duties, may lead to the termination of this

contract and/or other relationships with the Departments or Agencies that granted it access. [INSERT NAME OF CONTRACTOR] is aware that unauthorized release or mishandling of sensitive data may be grounds for adverse action against [INSERT NAME OF CONTRACTOR]. In addition, should [INSERT NAME OF CONTRACTOR] misuse records requiring protection under the Privacy Act, [INSERT NAME OF CONTRACTOR] has been advised that unauthorized disclosure of data protected by the Privacy Act may constitute a violation, or violations, of United States criminal law, and that Federally-affiliated workers (including some contract employees) who violate privacy safeguards may be subject to disciplinary actions, a fine up to \$5,000.00, or both.

4. [INSERT NAME OF CONTRACTOR] understands that all sensitive data to which [INSERT NAME OF CONTRACTOR] has access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government. [INSERT NAME OF CONTRACTOR] agrees that it must return all sensitive data which has, or may come into its possession or for which it is responsible because of such access:

- (a) upon demand by an authorized representative of the United States Government; or
- (b) upon the conclusion of the contract or other relationship that requires access to sensitive data.

Unless and until [INSERT NAME OF CONTRACTOR] is released in writing by an authorized representative of the United States Government, [INSERT NAME OF CONTRACTOR] understands that all conditions and obligations imposed upon it by this Agreement apply during the time [INSERT NAME OF CONTRACTOR] is granted access to sensitive data, and at all times thereafter.

5. In accordance with Public Law No. 108-447, Consolidated Act, 2005, the following is applicable:

These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including

sections 641, 793, 794, 798, and 952 of title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive order and listed statutes are incorporated into this agreement and are controlling.'

6. **[INSERT NAME OF CONTRACTOR]** further agrees:

(a) Signed Agreements. The Contractor further agrees to sign an agreement to this effect with other private or public entities providing proprietary data for performance under this contract. As part of this agreement, the Contractor will inform all parties of its agreement to allow certain Government designated contractors access to all data as described in paragraph (c) below. One copy of each signed agreement shall be forwarded to the Contracting Officer (CO).

(b) Government Designated Contractors. The Contractor agrees to allow the below listed Government-designated support contractors, possessing appropriate proprietary agreements and retained by the Government to advise the Government on cost, schedule and technical matters pertaining to this acquisition, access to any unlimited rights data acquired under the terms and conditions of this contract and to sign reciprocal nondisclosure agreements with them. One copy of each signed agreement shall be forwarded to the CO.

List designated contractors:

All Government-designated contractors stated herein, or added at a future date shall also enter into nondisclosure agreements with all parties providing proprietary information to the contractor.

(c) Remedy for Breach. The Contractor agrees that any breach or violation of the certifications or restrictions of this clause shall constitute a material and substantial breach of the terms, conditions and provisions of the contract and that the Government may, in addition to any other remedy available, terminate this contract for default in accordance with the provisions of FAR 52.249-6. Nothing in this clause or contract shall be construed to mean that the Government shall be liable to the owners of proprietary

information in any way for the unauthorized release or use of proprietary information by this contractor or its subcontractors.

GOVERNMENT WITNESS

THE EXECUTION OF THIS AGREEMENT WAS
WITNESSED BY THE UNDERSIGNED

[INSERT NAME OF ONTRACTOR]

BEFORE
ACCESSING SENSITIVE
DATA OF THE UNITED STATES
GOVERNMENT.

CONTRACTOR ACCEPTANCE

THE UNDERSIGNED ACCEPTED
AGREEMENT ON BEHALF OF

SIGNATURE

DATE

SIGNATURE

DATE

TITLE/POSITION:

TITLE/POSITION:

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

IN SUPPORT OF:

Department of Commerce (DOC)

Office of the Chief Information Officer (OCIO)

Office of IT Services (OITS)

NCR AAS Project Number ID11160043

1. PURPOSE

The QASP is a Government developed and applied document used to make sure that systematic quality assurance methods are used in the administration of this Performance Based Work Statement Contract (PBWSC). Standards identified in the Performance Requirements Summary in Attachment 1. The intent is to ensure that the Contractor performs in accordance with the performance metrics set forth, that the Government receives the quality of products/services called for in the contract and that the Government only pays for the acceptable products/services received.

This Quality Assurance Surveillance Plan (QASP) has been developed to evaluate contractor performance of the requirements set forth in the PWS. It is designed to provide an effective and systematic surveillance method of monitoring contractor performance for each Performance Requirements Summary (PRS).

The Contractor, and not the Government, is responsible for management and quality control actions to meet the terms of the task order. The role of the government is to promote quality assurance to ensure PRS standards are achieved.

The Contractor is required to develop a Quality Control Plan (QCP) that describes its method for measuring quality and plan for meeting or exceeding the Performance Requirements Summary (PRS) standards.

2. AUTHORITY

This QASP provides for the inspection and acceptance of products/services required in the task order. Inspection and acceptance will be accomplished by the Contracting Officer or his duly authorized representative.

3. SCOPE

The QASP contains the basis for inspection and acceptance of all of the products/services required under this task order.

4. GOVERNMENT RESOURCES

The following definitions for Government resources are applicable to this plan:

Contracting Officer (CO) - A person duly appointed with the authority to enter into, administer or terminate contracts and make related determinations and findings on behalf of the Government.

PPM/ GSA COR – An individual acting as the authorized representative of the CO for the technical administration of the task order.

5. RESPONSIBILITIES

The Government resources shall have responsibilities for the implementation of this QASP as follows:

Contracting Officer (CO) - The CO ensures performance of all necessary actions for the compliance with the terms of the task order and safeguards the interests of the United States in the contractual relationships. It is the CO that assures the Government receives impartial, fair and equitable treatment under this task order. The CO is ultimately responsible for the final determination of the adequacy of the Contractor's performance.

PPM/ GSA COR - The COR provides detailed technical oversight of the Contractor's performance. The COR will report to the CO as necessary in a timely, complete and impartial fashion to support the CO in the technical contract administration activities. While the COR may serve as a direct conduit to provide Government guidance and feedback to the Contractor on technical matters, he or she is not empowered to make any contractual commitments or to authorize any contractual changes on the Governments behalf. Any changes that the Contractor deems may affect contract, price, terms or conditions shall be referred to the CO for action.

6. METHODS OF QA SURVEILLANCE

The below listed methods of surveillance shall be used in the administration of this QASP. In addition to specific instructions that may be mentioned, the appropriate and standardized form that is to be used for documentation of a QA surveillance is the QASP/Surveillance Plan Checklist included in Attachment A.

Feedback – Feedback may be obtained either from surveys or from random customer complaints. To be considered valid, complaints must be set forth clearly and in writing the detailed nature of the complaint, must be signed and be forwarded to the CO and to the COR if warranted, The COR will maintain a summary log of all formally received complaints as well as a copy of each complaint in a documentation file. The COR shall also keep the results of all customer surveys on file and shall enter the summary results into the QASP/Surveillance Plan Checklist.

100% Inspection - This level of inspection shall be accomplished by monitoring and documentation. Each month the COR shall review the generated documentation and enter the summary results in the QASP/Surveillance Plan Checklist.

Periodic Inspection – Periodic inspection shall be conducted if and when specified in individual task orders. For the potential tasks that have been identified so far and included in this QASP, the appropriate COR typically performs the periodic inspection on a routine basis.

Random Monitoring – Random monitoring shall be conducted if and when specified in the task order. For the potential tasks that have been identified so far and included in this QASP, the random monitoring shall be performed by the COR and reported to the COR and recorded in the QASP/Surveillance Plan Checklist as appropriate.

ATTACHMENT 1: PERFORMANCE REQUIREMENTS SUMMARY

REQUIRED SERVICES (TASKS/DELIVERABLES)	PERFORMANCE STANDARDS	ACCEPTABLE QUALITY LEVELS	METHODS OF SURVEILLANCE
Transition In Plan – Draft	Due at Kickoff Meeting	95% of the time	100% Inspection Document Review
Transition In Plan - Final	10 Days after receipt of Government Comments	95% of the time	100% Inspection Document Review
Transition Out Plan Draft	NLT 90 days before Task Order expiration	95% of the time	100% Inspection Document Review
Transition Out Plan - Final	10 Days after receipt of Government Comments	95% of the time	100% Inspection Document Review
Kickoff Meeting	Within 5 days of award	95% of the time	100% Inspection Document Review
Monthly Status Reports	Monthly, 10th calendar day of the next month	95% of the time	100% Inspection Document Review
Weekly Technical Status Report	Weekly, Wednesday by 9:30 a.m.	95% of the time	100% Inspection Document Review
Project Management Plan - Draft	NLT 20 days after kickoff meeting and then annually for updates	95% of the time	100% Inspection Document Review
Project Management Plan - Final	10 days after receipt of Government Comments	95% of the time	100% Inspection Document Review
Project Management Plan Updates	At least annually	95% of the time	100% Inspection Document Review
QCP - Draft	NLT 20 days after kickoff meeting	95% of the time	100% Inspection Document Review
QCP - Final	10 Days after receipt of Government Comments	95% of the time	100% Inspection Document Review
QCP - Updates	At least annually	95% of the time	100% Inspection Document Review
Network Hardware Installation Documentation	At the time of Installation	95% of the time	100% Inspection Document Review
Network Maintenance Documentation	Prior to Network Maintenance Activity	95% of the time	100% Inspection Document Review
Network Infrastructure Diagrams and AutoCad Drawings	NLT 10 days after changes are made	95% of the time	100% Inspection Document Review
Network, VOIP, and EBS Performance Statistical Reports	Weekly, Monthly, Quarterly	95% of the time	100% Inspection Document Review
Vulnerability scanning and reporting	Monthly	95% of the time	100% Inspection Document Review
Work Breakdown Structure	NLT 10 days after need is identified	95% of the time	100% Inspection Document Review
Network Engineering Studies, Design	NLT 20 days after optional	95% of the time	100% Inspection

and Engineering Plan for Virtual Server Migration	CLIN is exercised		Document Review
New Technical Architecture Documentation	NLT 10 days after emerging technology is identified	95% of the time	100% Inspection Document Review
Provide archived versions of events and viewer data	NLT 10 days after event	95% of the time	100% Inspection Document Review
Daily Health Check	Daily	95% of the time	Periodic Inspection
Software and Hardware Test Result Documentation	Prior to Implementing Any Change	95% of the time	100% Inspection Document Review
System Performance and Utilization Reports	Weekly, Monthly, Quarterly	95% of the time	Periodic Inspection
New Technology Recommendations	As New Technology Becomes Available	95% of the time	Periodic Inspection
Standard Operating Procedure Updates	As appropriate as changes are made	95% of the time	100% Inspection Document Review
Initial IT Security Orientation Training	NLT 10 days after task order award	95% of the time	100% Inspection Document Review
Provisions Acknowledgment	NLT 10 days after task order award	95% of the time	100% Inspection Document Review
System Certification Work Plan	NLT 14 days after task order award	95% of the time	100% Inspection Document Review
System Security Plan and Certification Documentation	NLT 14 days after approval from Government	95% of the time	100% Inspection Document Review
Invoices	Invoices are accurate (i.e. amounts, backup documentation) and submitted on the 10 th of each month	95% of the time	Monthly surveillance
Deliverables and Reports. The contractor submits all deliverables outlined in the contract.	95% accuracy of the deliverables/reports and are corrected within five business days. The remaining 5% of the documented discrepancies cause no slip in schedule.	95% resolved in 10 days. No slip in schedule.	Periodic surveillance

**ATTACHMENT 2: Monthly Evaluation of Contractor's Performance
For**

Task Order: _____

Contractor _____ Evaluation Period: _____
Contract #: _____ Task Order #: _____
Method of surveillance: _____

The contractor shall be evaluated monthly using the following ratings:

3 = Excellent: Contractor exceeded performance requirements

2 = Satisfactory: Contractor met performance requirements.

1 = Unsatisfactory: Contractor did not meet all performance requirements.

1. Submittal of Deliverables – Contractor personnel's work is timely.

Rating: 1 _____ 2 _____ 3 _____

Comments:

2. Quality of Work of Deliverables – Contractor personnel's work is complete and accurate.

Rating: 1 _____ 2 _____ 3 _____

Comments:

3. Contractors' adherence to security requirements as required in the task order.

Rating: 1 _____ 2 _____ 3 _____

Comments:

Additional Comments:

Name of Evaluator: _____

Title of Evaluator: _____

Phone Number: _____

Signature: _____

Date: _____

Reading rooms located at Department of Commerce (DOC) (1401 Constitution Ave, NW, Washington, DC 20230) will be made available to all Alliant Small Business prime contractors for the purpose of reviewing proprietary materials, guides, manuals, and documents pertinent to understanding the services and requirements under this procurement. Potential and interested subcontractors must accompany an Alliant Small Business prime contractor for viewing purposes. The rooms will be available between April 10th and April 17th. Please contact the following individuals to schedule:

Kevin Carpenter; kcarpenter@doc.gov; 202-482-0982

Charlene Grant; cgrant@doc.gov; 202-482-4444

Wes Ky; wky@doc.gov; 02-482-6038

The following rules will apply to all contractors. **Failure to fully comply could result in a contractor's disqualification for consideration on this requirement.**

1. Rooms can be reserved for one (1) four hour block during the following times; 7:30am to 1:00 pm and 1:30pm – 5:00pm EST daily. Contractors are restricted to reserving a room for no more than four hours total.
2. Contractors are allowed up to 5 individuals in the reading room to review documents;
3. No cellular phones, cameras, computers, or recording devices are permitted inside a reading room;
4. A confidentiality agreement must be executed by each member of the contractor's review team. DOC will provide the agreement via e-mail at the time of reservation. The signed agreement(s) must be presented prior to accessing the reading room. In addition, a copy of the signed agreement(s) must be email to the contracting office at daniel.r.miller@gsa.gov and Julius.bradshaw@gsa.gov;
5. Documents shall not be removed from the room;
6. The use of paper and pen are allowed.

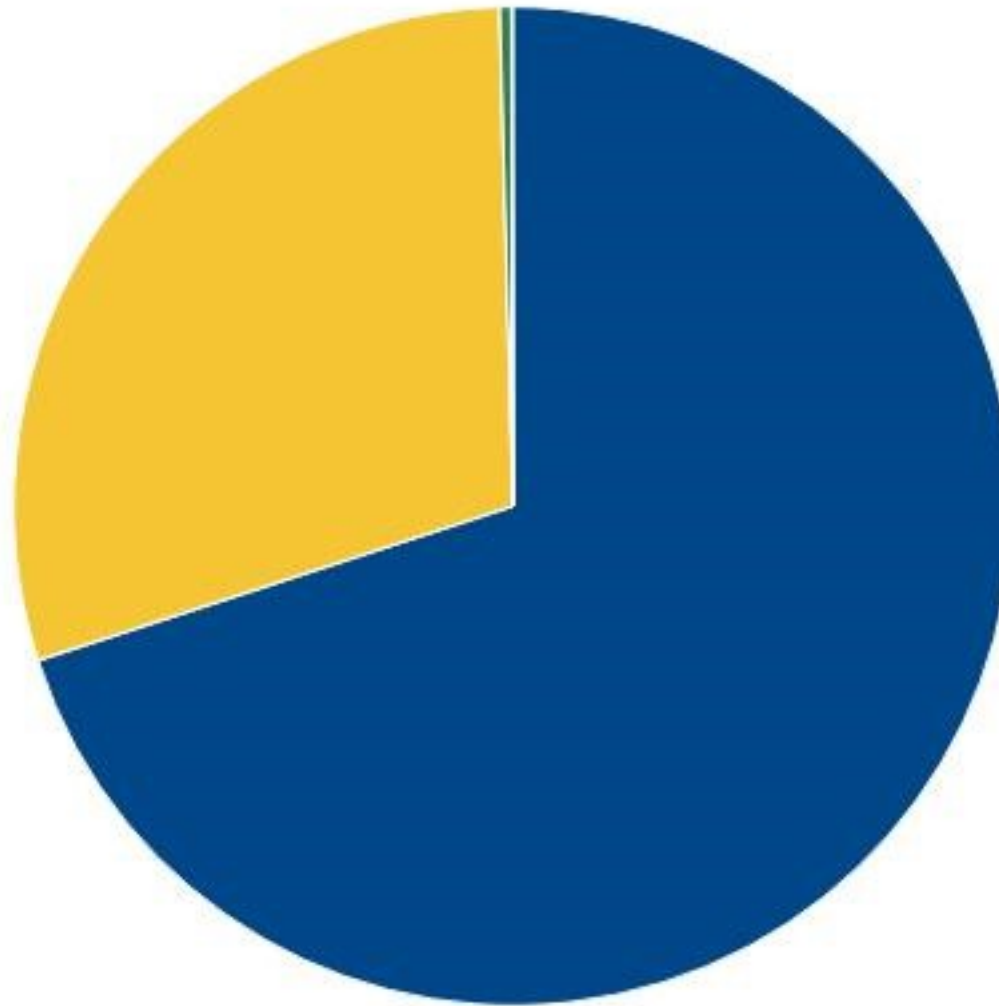
DOC will provide the following materials, guides, manuals, and documents in the reading room:

- System Security Plans
- NOC Standard Operating Procedures Register with dates that they were last updated
- SOC Standard Operating Procedures Register with dates that they were last updated
- HCHBNet Equipment that have been recently refreshed and/or slated for refresh this Phase 3
- MTIPS Bandwidth Utilization Report for the past 90 days
- HCHBNet Network Diagram (sanitized PDF version) to include remote sites connectivity
- NOC and SOC Daily Checklist
- Typical Access Layer Switch Configuration
- Typical Distribution and Core Switches Configuration
- Security Hardening Guideline or procedures for hardening servers and network equipment
- Mass Notification System or EBS As-Built Diagrams
- EBS Testing Procedure depicting how often we conduct testing and how do we remedy issues

- VoIP and Analog Lines Count (most recent report)
- Network Nodes Count (most recent report)
- HCHBNet After Actions Report Template
- NOC and SOC Maintenance Renewal Spreadsheet

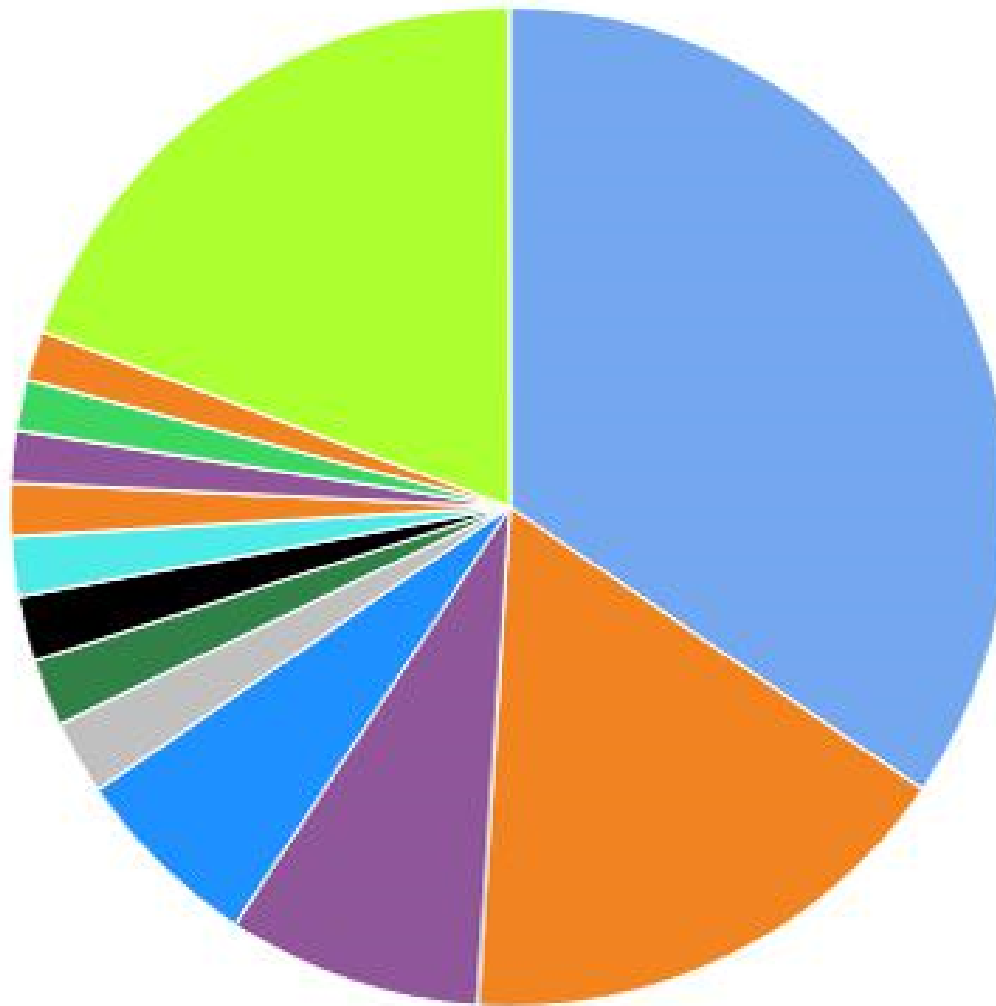
Function	Initiative	Description	Support Type
Infrastructure Operations	Security Operations & Maintenance	Network Intrusion Detection and Prevention Support/Renewal	Hardware
Infrastructure Operations	Security Operations & Maintenance	WebSense Hardware Support	Hardware
Infrastructure Operations	Infrastructure Support	APC Maintenance Data Center	Maintenance
Infrastructure Operations	Security Operations & Maintenance	Security Information and Event Monitoring Software (McAfee/Nitro)	Maintenance
Infrastructure Operations	Server Virtualization Environment	VSPHERE 64 licenses for Processor	Maintenance
Infrastructure Operations	Infrastructure Support	Vcloud Automation Center	Maintenance
Infrastructure Operations	Infrastructure Support	APC NetBotz Datacenter Maintenance Renewal	Maintenance
Infrastructure Operations	Infrastructure Support	Comm Vault simpna 10	Maintenance
Infrastructure Operations	Infrastructure Support	619 RSA Tokens	Hardware
Infrastructure Operations	Infrastructure Support	150 RSA Tokens	Hardware
Infrastructure Operations	Infrastructure Support	RSA Authentication Manager	Maintenance
Infrastructure Operations	Infrastructure Support	ServiceNow Licenses	Maintenance
Infrastructure Operations	Security Operations & Maintenance	Vulnerability Scan and Management Licensing (Tenable)	Maintenance
Infrastructure Operations	Infrastructure Support	Men & Mice	Maintenance
Infrastructure Operations	Infrastructure Support	DNSSEC Software	Maintenance
Infrastructure Operations	Infrastructure Support	symantec backup	Maintenance
Infrastructure Operations	Infrastructure Support	Infotel Call Accounting	Maintenance
Infrastructure Operations	Infrastructure Support	Solarwinds Orion Network Performance Monitor	Maintenance
Infrastructure Operations	Infrastructure Support	SSL Certificate for Wireless	Maintenance
Infrastructure Operations	Infrastructure Support	Entrust SSL Certificate	Maintenance
Infrastructure Operations	Infrastructure Support	SolarWinds Virtual Manager	Maintenance
Infrastructure Operations	Infrastructure Support	SolarWinds Network Configuration Manager	Maintenance
Infrastructure Operations	Infrastructure Support	SolarWinds User Device Tracker v3	Maintenance
Infrastructure Operations	Infrastructure Support	Solarwinds Orion Network Traffic Analyzer	Maintenance
Infrastructure Operations	Infrastructure Support	Callrex call center software	Maintenance
Infrastructure Operations	Infrastructure Support	SolarWinds IP Address Manager	Maintenance
Infrastructure Operations	Infrastructure Support	Solarwinds VOIP and Network Quality Manager	Maintenance
Infrastructure Operations	Infrastructure Support	Solarwinds Engineer Toolset for desktop	Maintenance
Infrastructure Operations	Infrastructure Support	Airmagnet wireless survey tool	Maintenance
Infrastructure Operations	Infrastructure Support	LANDesk	Maintenance
Infrastructure Operations	Infrastructure Support	Hitachi ID Password Manager	Maintenance
Infrastructure Operations	Infrastructure Support	ProofPoint Anti-Spam	Maintenance
Infrastructure Operations	Infrastructure Support	Quest License Renewal	Maintenance
Infrastructure Operations	Infrastructure Support	ActivIdentity	Maintenance

All Incidents by Priority for Last Year

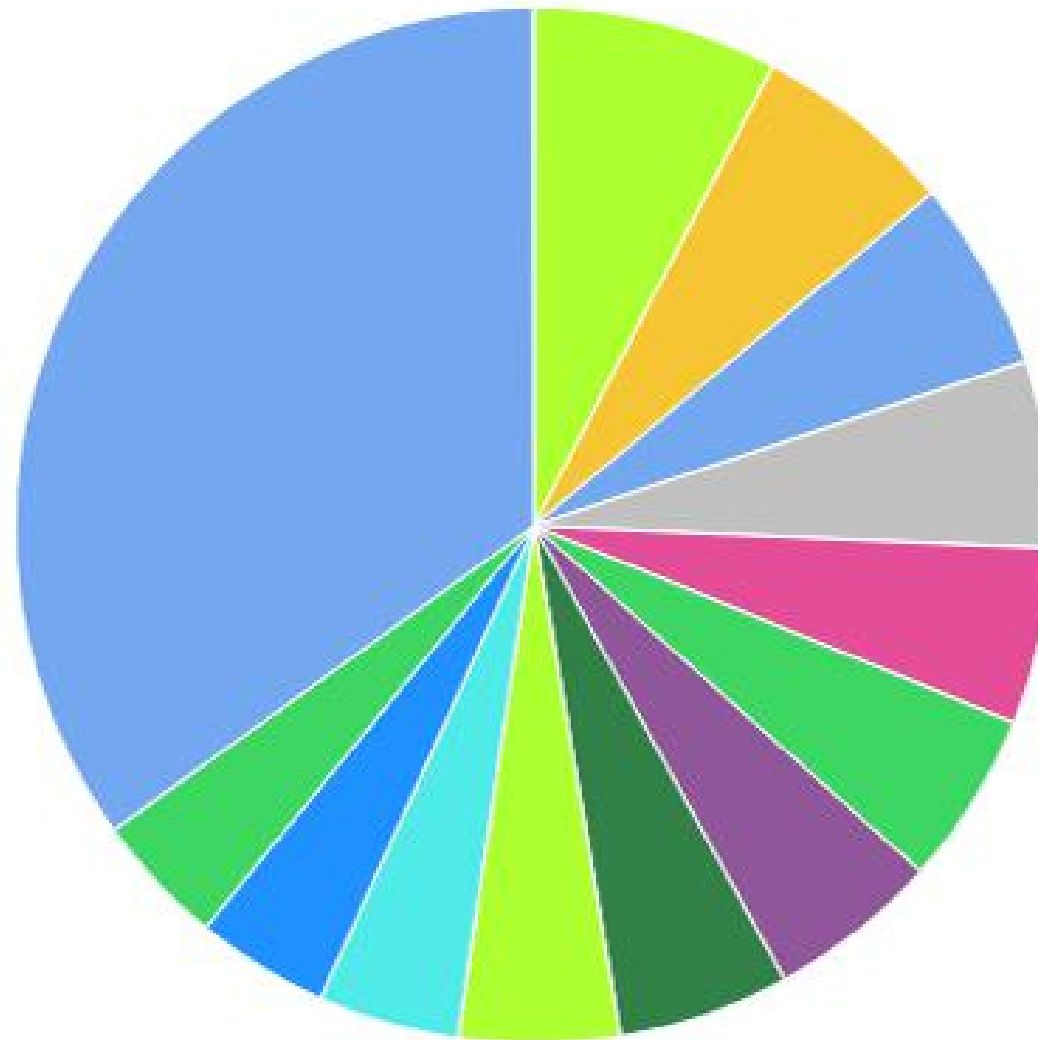


4 - Low = 17,102 (70.01%)	3 - Moderate = 7,225 (29.58%)	2 - High = 92 (0.38%)
1 - Critical = 9 (0.04%)		

All Incidents by Category for Last Year



Accellion Sft = 7,682 (34.56%)	Windows = 3,661 (16.47%)	(empty) = 1,831 (8.24%)
Outlook = 1,367 (6.15%)	Printer = 538 (2.42%)	Authentication = 486 (2.19%)
McAfee EPO = 464 (2.09%)	AnyConnect = 434 (1.95%)	Network = 379 (1.71%)
Other = 379 (1.71%)	iPhone = 363 (1.63%)	SSL VPN = 362 (1.63%)
Other (more ...) = 4,280 (19.26%)		



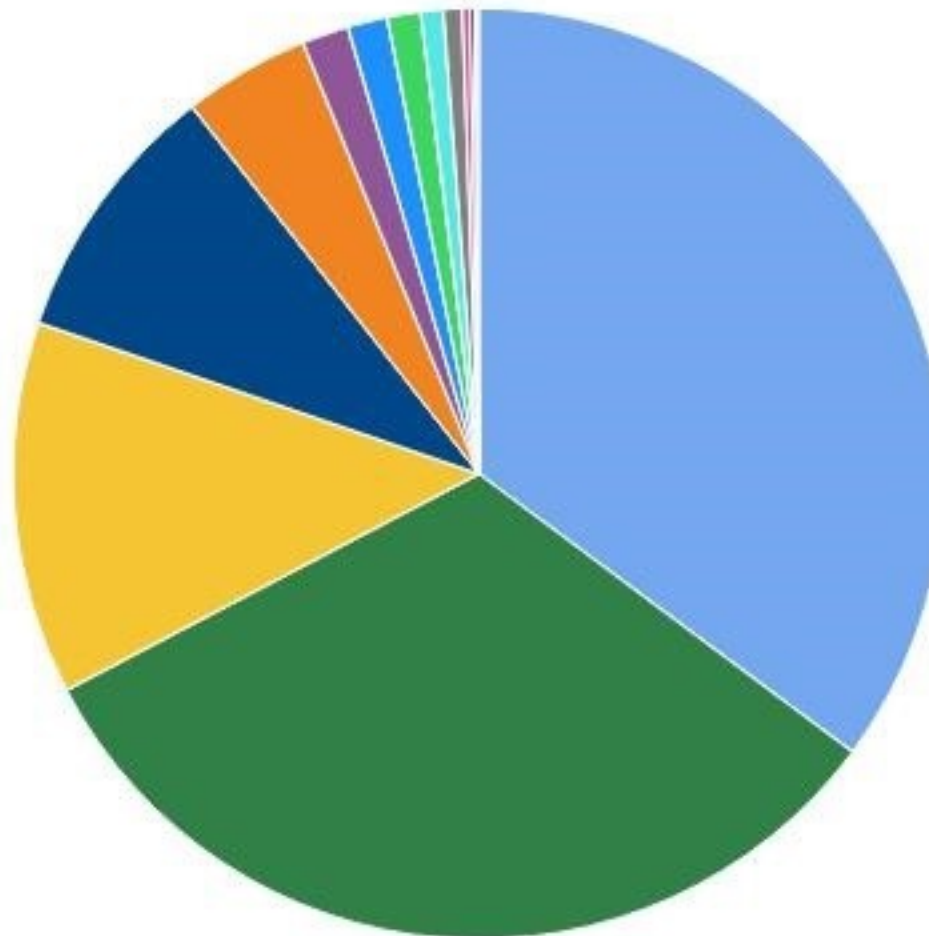
Laptop = 327 (1.47%)	Uncategorized = 269 (1.21%)	ServiceNow = 254 (1.14%)
Endpoint = 249 (1.12%)	Office = 237 (1.07%)	VPN Token = 231 (1.04%)
Android Smartphone = 230 (1.03%)	Citrix = 229 (1.03%)	Access = 215 (0.97%)
Java = 188 (0.85%)	Reset Pin = 178 (0.80%)	OPCS = 176 (0.79%)
		Other = 1,497 (6.74%)

All_Incidents_ResolutionbyTier_LastYear

Service Desk = Tier 1

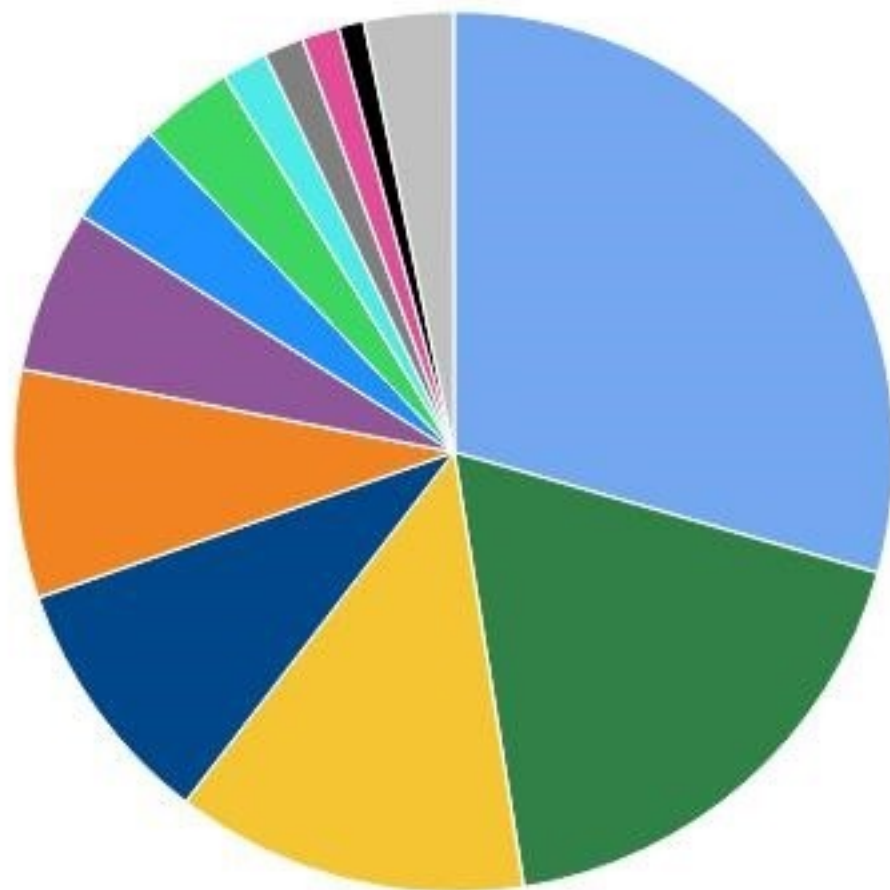
Desk Side = Tier 2

All Others = Tier 3



Service Desk = 9,403 (35.19%)	LAN = 8,584 (32.12%)	Sunflower = 3,460 (12.95%)
Desk-side = 2,451 (9.17%)	NOC = 1,174 (4.39%)	CIRT = 436 (1.63%)
SOC = 310 (1.16%)	OSY = 209 (0.78%)	EDA = 174 (0.65%)
ServiceNow Admins = 41 (0.15%)	Other = 36 (0.13%)	Shared Services AV = 72 (0.27%)
Comprizon = 371 (1.39%)		

All Requests by Category for Last Year



DOC Pre-Travel Request = 139 (1.68%) DOC Post-Travel Request = 121 (1.47%)
Employee Move = 112 (1.36%) Call Forwarding Request = 78 (0.94%) Other = 271 (3.28%)

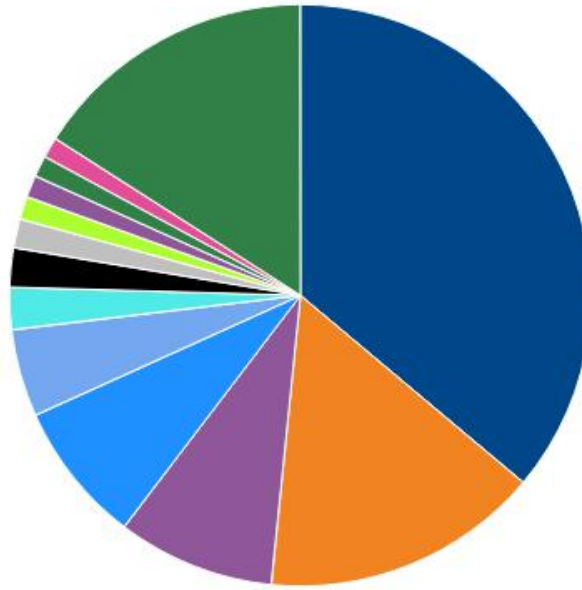
▲ 2/2 ▼

Employee Access Request = 2,429 (29.43%) Telephone Configuration Request = 1,490 (18.05%)
Install/Remove My Hardware Request = 1,069 (12.95%) Software Request = 760 (9.21%)
New Employee Setup Request = 693 (8.40%) Employee Departure Request = 494 (5.98%)
Port Activation Request = 317 (3.84%) Loaner Request = 281 (3.40%)

▲ 1/2 ▼

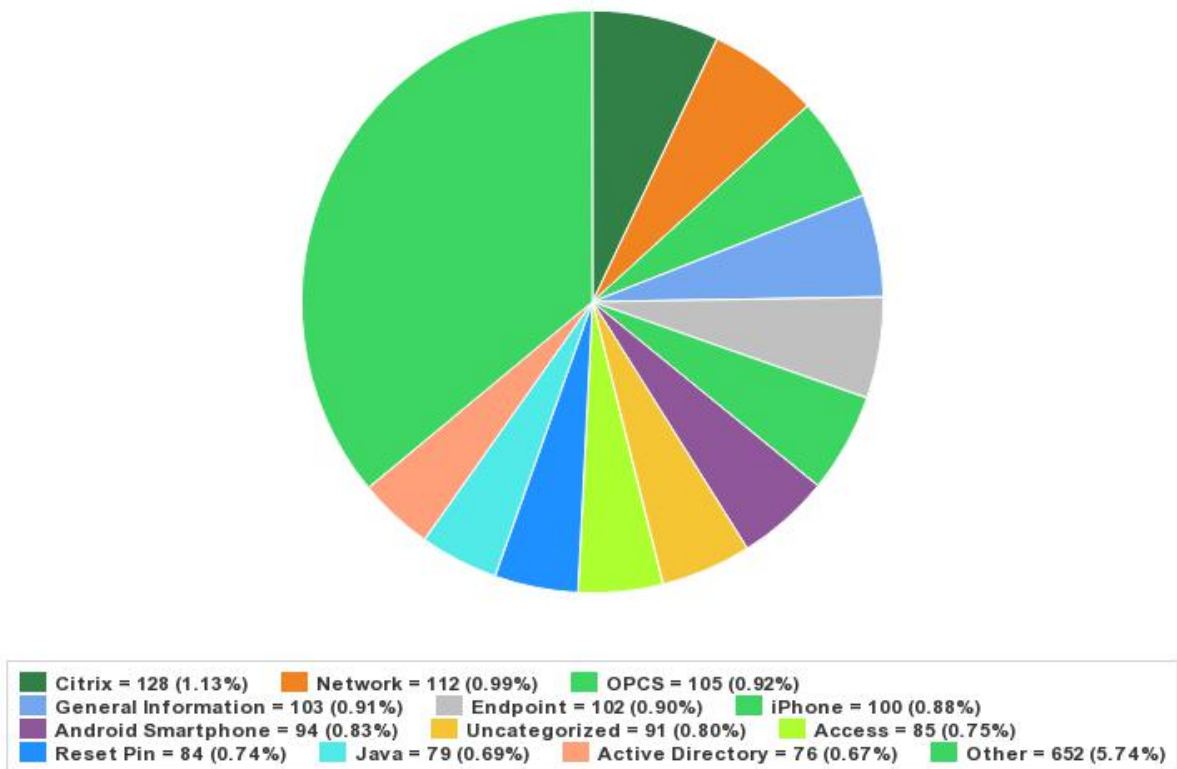
DOC ITSD Last 6 Months Tickets by Category

All Incidents by Category for Last Six Months



Accellion SFT = 4,107 (36.13%)	Windows = 1,760 (15.48%)	(empty) = 995 (8.75%)
Outlook = 895 (7.87%)	Authentication = 554 (4.87%)	AnyConnect = 266 (2.34%)
McAfee EPO = 248 (2.18%)	Printer = 183 (1.61%)	Laptop = 145 (1.28%)
ServiceNow = 134 (1.18%)	Office = 131 (1.15%)	Other (more ...) = 1,811 (15.93%)
		Other = 139 (1.22%)

All Incidents by Category for Last Six Months - Page 2



Breakdown of the “Other” category.

Month and Year	Help Desk Abandonment	Help Desk Total
Oct-17	175	1635
Nov-17	105	1482
Dec-15	179	1360
Jan-16	336	1427
Feb-16	148	1483
Mar-16	255	1638
Apr-16	356	1460
May-16	300	1615
Jun-16	233	1730
Jul-16	149	1514
Aug-16	234	1795
Sep-16	454	1754

Abandonment Rate

11%

7%

13%

24%

10%

16%

24%

19%

13%

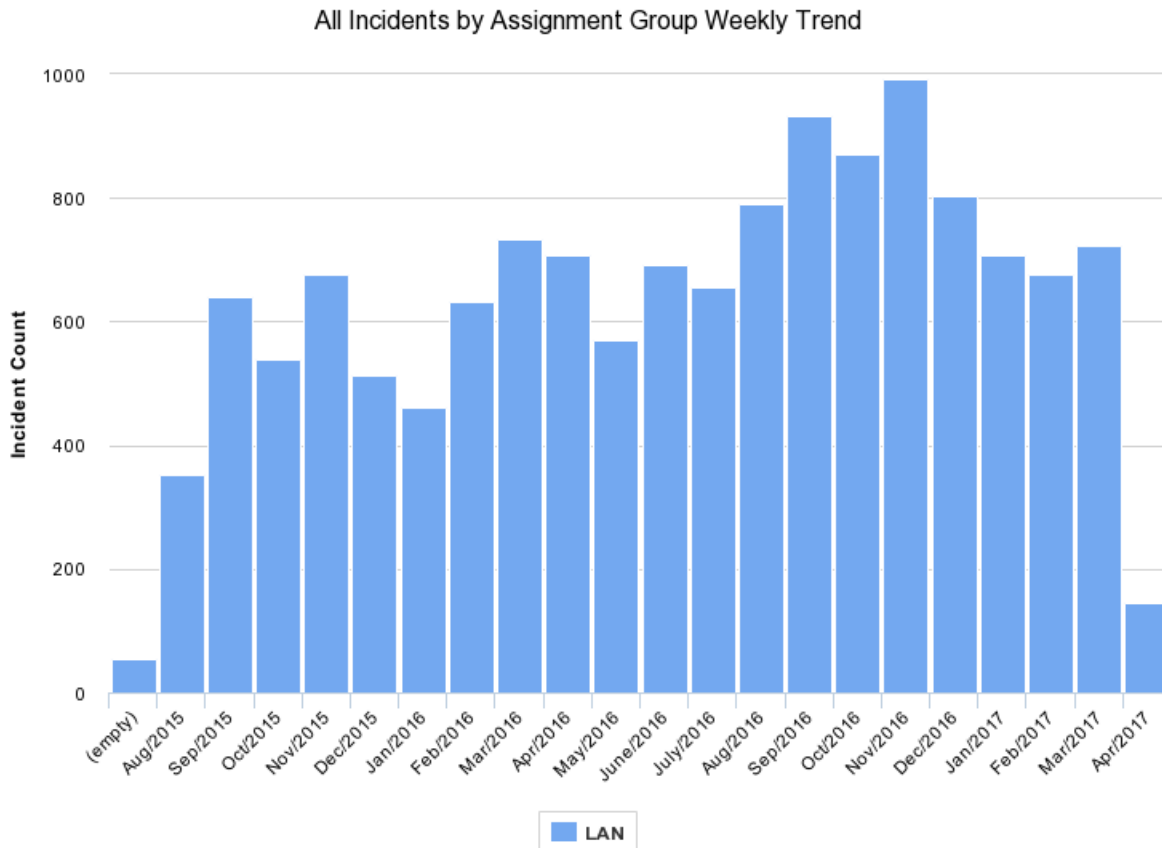
10%

13%

26%

All Incidents by Assignment Group Weekly
Trend

Report Title: All Incidents by Assignment Group Weekly Trend
Run Date and Time: 2017-04-06 12:46:37 Eastern Standard Time
Run By: XXXXXXXXXX
Table name: incident
Query Condition: Assignment group = LAN
Group by: Assignment group



Created Totals	Count Totals	Percent
(empty) Total	54	0.39%
Aug/2015 Total	352	2.54%
Sep/2015 Total	640	4.62%
Oct/2015 Total	540	3.89%
Nov/2015 Total	675	4.87%
Dec/2015 Total	513	3.70%
Jan/2016 Total	462	3.33%
Feb/2016 Total	632	4.56%
Mar/2016 Total	733	5.29%
Apr/2016 Total	708	5.11%

All Incidents by Assignment Group Weekly
Trend

Created Totals	Count Totals	Percent
May/2016 Total	571	4.12%
June/2016 Total	693	5.00%
July/2016 Total	656	4.73%
Aug/2016 Total	791	5.70%
Sep/2016 Total	933	6.73%
Oct/2016 Total	870	6.27%
Nov/2016 Total	991	7.15%
Dec/2016 Total	803	5.79%
Jan/2017 Total	707	5.10%
Feb/2017 Total	676	4.87%
Mar/2017 Total	723	5.21%
Apr/2017 Total	144	1.04%

Created	Assignment group	Count	Percent
(empty)	LAN	54	100.00%
Aug/2015	LAN	352	100.00%
Sep/2015	LAN	640	100.00%
Oct/2015	LAN	540	100.00%
Nov/2015	LAN	675	100.00%
Dec/2015	LAN	513	100.00%
Jan/2016	LAN	462	100.00%
Feb/2016	LAN	632	100.00%
Mar/2016	LAN	733	100.00%
Apr/2016	LAN	708	100.00%
May/2016	LAN	571	100.00%

All Incidents by Assignment Group Weekly
Trend

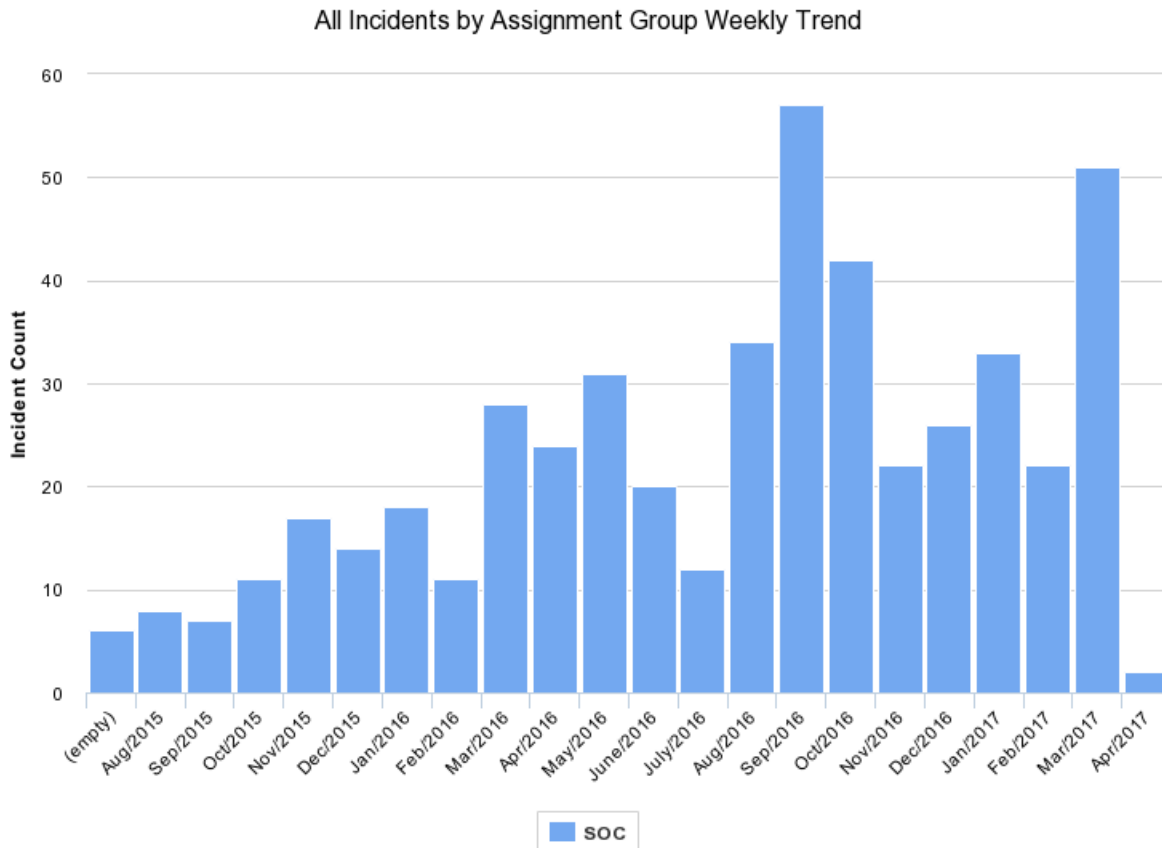
Created	Assignment group	Count	Percent
June/2016	LAN	693	100.00%
July/2016	LAN	656	100.00%
Aug/2016	LAN	791	100.00%
Sep/2016	LAN	933	100.00%
Oct/2016	LAN	870	100.00%
Nov/2016	LAN	991	100.00%
Dec/2016	LAN	803	100.00%
Jan/2017	LAN	707	100.00%
Feb/2017	LAN	676	100.00%
Mar/2017	LAN	723	100.00%
Apr/2017	LAN	144	100.00%
Total		13,867	

Network Port Activation: Moves, Adds, and Changes Historical Tickets

Month	Tickets Count
Mar-16	109
Apr-16	84
May-16	70
Jun-16	95
Jul-16	96
Aug-16	104
Sep-16	101
Oct-16	70
Nov-16	103
Dec-16	81
Jan-17	103
Feb-17	105
Mar-17	45
Total	1166

All Incidents by Assignment Group Weekly
Trend

Report Title: All Incidents by Assignment Group Weekly Trend
Run Date and Time: 2017-04-06 12:43:03 Eastern Standard Time
Run By: XXXXXXXXXX
Table name: incident
Query Condition: Assignment group = SOC
Group by: Assignment group



Created Totals	Count Totals	Percent
(empty) Total	6	1.21%
Aug/2015 Total	8	1.61%
Sep/2015 Total	7	1.41%
Oct/2015 Total	11	2.22%
Nov/2015 Total	17	3.43%
Dec/2015 Total	14	2.82%
Jan/2016 Total	18	3.63%
Feb/2016 Total	11	2.22%
Mar/2016 Total	28	5.65%
Apr/2016 Total	24	4.84%

All Incidents by Assignment Group Weekly
Trend

Created Totals	Count Totals	Percent
May/2016 Total	31	6.25%
June/2016 Total	20	4.03%
July/2016 Total	12	2.42%
Aug/2016 Total	34	6.85%
Sep/2016 Total	57	11.49%
Oct/2016 Total	42	8.47%
Nov/2016 Total	22	4.44%
Dec/2016 Total	26	5.24%
Jan/2017 Total	33	6.65%
Feb/2017 Total	22	4.44%
Mar/2017 Total	51	10.28%
Apr/2017 Total	2	0.40%

Created	Assignment group	Count	Percent
(empty)	SOC	6	100.00%
Aug/2015	SOC	8	100.00%
Sep/2015	SOC	7	100.00%
Oct/2015	SOC	11	100.00%
Nov/2015	SOC	17	100.00%
Dec/2015	SOC	14	100.00%
Jan/2016	SOC	18	100.00%
Feb/2016	SOC	11	100.00%
Mar/2016	SOC	28	100.00%
Apr/2016	SOC	24	100.00%
May/2016	SOC	31	100.00%

All Incidents by Assignment Group Weekly
Trend

Created	Assignment group	Count	Percent
June/2016	SOC	20	100.00%
July/2016	SOC	12	100.00%
Aug/2016	SOC	34	100.00%
Sep/2016	SOC	57	100.00%
Oct/2016	SOC	42	100.00%
Nov/2016	SOC	22	100.00%
Dec/2016	SOC	26	100.00%
Jan/2017	SOC	33	100.00%
Feb/2017	SOC	22	100.00%
Mar/2017	SOC	51	100.00%
Apr/2017	SOC	2	100.00%
Total		496	



Department of Commerce

Commerce Information

CITR-017

Technology Requirement

January 25, 2012

Security Configuration Checklist Program

1. PURPOSE

This policy provides Information Technology Security Program Policy (ITSP) requirements for the Department of Commerce (DOC) Operating Unit (OU) Security Configuration Checklist Programs.

2. BACKGROUND

A comprehensive Security Configuration Checklist Program consisting of asset inventory, and automated assessment processes, ensures that information technology (IT) system security controls remain effective over time. In 2008, the Office of Management and Budget (OMB) issued Memorandum M-08-22, "*Guidance on the Federal Desktop Core Configuration (FDCC)*" which requires the use of Security Content Automation Protocol (SCAP) validated tools to scan for FDCC configurations. OMB also issued Memorandum M-11-33, "*FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*" which includes requirements to: 1) report IT asset inventory information using an automated capability that produces SCAP compliant output; and 2) provide the number of IT assets where an automated configuration capability produces SCAP compliant output. When planning for the implementation of this policy, OUs are also advised to consider CITR-016 on the subject of Vulnerability Scanning and Patch Management.

3. SCOPE

These requirements apply to all unclassified information systems owned by or operated on behalf of DOC where the Department has the legal and/or contractual authority to dictate requirements.

4. AUTHORITY

The DOC Chief Information Officer (CIO) has the authority to develop, implement, and manage IT security processes and procedures to protect the availability, confidentiality, and integrity of the Department's IT resources. The DOC Chief Information Security Officer (CISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and FISMA; with regulatory requirements and external guidance, including OMB policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirements.

5. CANCELLATION/AUGMENTATION OF EXISTING POLICY

This policy augments ITSPS sections 4.5.1, “*Baseline Configuration*,” and supersedes CTR-001, “Federal Desktop Core Configuration (FDCC).”

6. REQUIREMENTS

The IT Security Configuration Checklist Program is comprised of the following: asset inventory, configuration scanning and checklist requirements, and program management requirements.

A. Asset Inventory Requirements

1. Automated mechanisms must be used to develop and maintain asset inventories of network-connected IT devices.
2. Asset inventories for network-connected IT devices must include the network address, IT device type, and system software release and patch levels.
3. In circumstances where automated inventory mechanisms are not available, manual system inventories must be maintained for IT devices that are not network-connected.

B. Configuration Scanning and Checklist Requirements

1. OUs must identify secure configuration checklists for IT devices documented in their asset inventories and utilize these checklists to perform configuration scanning on IT devices. Results from scanning shall be analyzed and device configurations modified to align with the specified checklist.
2. Configuration checklists from the FDCC and United States Government Configuration Baseline (USGCB) must be utilized for configuration scanning.¹ Configuration scanning must be done on a monthly basis. For platforms not covered by FDCC and USGCB, checklists should be identified for use in accordance with the recommendations of NIST SP 800-70, “National Checklist Program for IT Products – Guidelines for checklist Users and Developers”, with priority given to checklists from the NIST Checklist Repository.
3. When available, OUs shall use configuration scanning tools that produce SCAP-compliant output.

C. Program Management Requirements

1. Authorizing Officials (AO) or their designees shall manage, accept and document risks introduced when the security configuration checklist program requirements cannot be performed.

¹ OU ITSOs may authorize deviations from the FDCC and USGCB. A copy of deviations must be maintained by the OU CIO.

2. OUs must maintain an OU-level checklist repository to make checklists available to system owners. The Department will be provided with access to this repository as required for oversight and compliance reviews.
3. Per the DOC ITSP, OUs are required to comply with CITRs within 90 days, or as stipulated in the CTR. Compliance with CTR requirements beyond the specified timeframe shall be managed through the Plans of Action and Milestones (POA&Ms).

7. REFERENCES

M-08-22, Memorandum for the Chief Information Officers Guidance on the Federal Desktop Core Configuration (FDCC)

<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-22.pdf>

M-11-33, Memorandum for Heads of Executive Departments and Agencies FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf>

NIST, National Checklist Program for IT Products – Guidelines for checklist Users and Developers

<http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf>

Simon Szykman

Chief Information Officer